De organisatie van botnetbestrijding in Nederland

TIMO SCHLESS

STUDENTNR. 838808421

10 september 2013

The Organisation of Counter Botnet Activities in The Netherlands

TIMO SCHLESS

STUDENTNR. 838808421

10 september 2013

Open Universiteit, faculteiten Managementwetenschappen en Informatica
Masteropleiding Business Process Management and IT

T9232B

1e begeleider en examinator:
dr.ir. H.P.E. (Harald) Vranken

2e begeleiders:
dr.ir. A.J.F. (Arjan) Kok en dr. A.D. (Anda) Counotte-Potman

Samenvatting

Botnets zijn netwerken van geïnfecteerde computers en mobiele apparaten, zogenaamde '*bots*', die onder controle staan van iemand die er gecoördineerde aanvallen op computersystemen mee uitvoert. De grootte van een botnet kan variëren van enkele honderden tot vele duizenden computers. Door gebruik te maken van zoveel computers blijft de eigenlijke aanvaller anoniem, terwijl hij tegelijk een groot computerpotentieel tot zijn beschikking heeft. Omdat botnets een grote dreiging vormen voor overheden, bedrijven en particulieren die gebruik maken van het internet, is het van belang ze te bestrijden. Dit onderzoek heeft tot doel om vast te stellen of de bestrijding van botnets in Nederland zodanig is georganiseerd dat daarmee de bestrijding van botnets effectief mogelijk is. De centrale onderzoeksvraag luidt:

Is de bestrijding van botnets organisatorisch effectief ingericht in Nederland?

Het onderzoek is uitgevoerd in een theoretisch en empirisch deel. Het theoretisch deel van het onderzoek had tot doel om op basis van literatuuronderzoek een conceptueel model en een referentiemodel vast te stellen die weergeven welke soorten partijen met welke competenties en bevoegdheden nodig zijn bij de bestrijding van botnets. Het literatuuronderzoek is uitgevoerd aan de hand van vier onderzoeksvragen:

De eerste theoretische onderzoeksvraag richtte zich op welke soorten botnets op basis van hun eigenschappen kunnen worden onderscheiden. Daarvoor is gekeken naar de kenmerkende aspecten van botnets om op basis daarvan in kaart te brengen of de betrokken organisaties in Nederland over de benodigde competenties en bevoegdheden beschikken om botnets te bestrijden. Botnets kennen veel verschijningsvormen en gradaties van complexiteit. Er bestaan relatief eenvoudige centrale commandostructuren, waarbij een centrale server de bots aanstuurt. Maar er zijn ook complexere vormen met een decentrale commandostructuur waarbij de bots een *peer-to-peer* netwerk vormen. Wanneer deze vormen worden gecombineerd met gebruik van sociale media en clouddiensten, ontstaat er een complexe hybride structuur. De intentie kan variëren van cybervandalisme tot cybercrime, hacktivisme, cyberterrorisme en cyberoorlog.

Met de tweede theoretische onderzoeksvraag is onderzocht welke methoden kunnen worden onderscheiden voor de bestrijding van botnets. De bestrijdingsmethoden zijn in te delen in methoden die individuele bots bestrijden, methoden die de botnetstructuur aangrijpen en methoden die zich richten op de botmaster. Het is hierbij van belang te beseffen dat er geen allesomvattende methode voor de detectie, analyse en bestrijding van botnets bestaat. Afhankelijk van de opzet en complexiteit van het botnet, is altijd een combinatie van methoden nodig om een botnet op te sporen, in kaart te brengen en te bestrijden.

Aan de hand van de derde en vierde theoretische onderzoeksvraag zijn de benodigde competenties en bevoegdheden voor botnetbestrijding in kaart gebracht, evenals de organisaties die bij de bestrijding zijn betrokken. Negentien competenties blijken nodig voor de detectie en analyse van botnets, en het aangrijpen van bots, botnetstructuren en botmasters. Er is echter geen individuele publieke of private organisatie die over al deze competenties beschikt of bevoegd is deze competenties aan te wenden.

Op basis van de uitkomsten van de literatuurstudie, is de samenhang tussen competenties en bevoegdheden van de organisaties die in Nederland betrokken zijn bij botnetbestrijding nader uitgewerkt en gevat in een referentiemodel. Dit model laat zien over welke competenties en bevoegdheden ieder van de betrokken organisaties zou moeten beschikken om gezamenlijk in staat te zijn alle soorten botnets, ingedeeld naar intentie en commandostructuur, te bestrijden. Het model voorspelt dat er binnen Nederland een hiaat is in de bevoegdheden voor effectieve botnetbestrijding, omdat benodigde competenties voor botnetbestrijding, gezien de aard van het fenomeen, niet volledig in de klassieke taken en bevoegdheden van betrokken overheidsorganisaties passen. Dit hiaat zit vooral in het wettelijke verbod om een commandoserver of de communicatie van een botnet over te nemen, het zogenaamde 'terughacken'.

Het empirisch deel van het onderzoek heeft vervolgens getoetst of het referentiemodel – dat op basis van noodzakelijke competenties en bevoegdheden weergeeft welke partijen er betrokken zijn bij de bestrijding van botnets – overeenkomt met de wijze waarop in Nederland de botnetbestrijding is georganiseerd. Met een semigestructureerd interview, gebaseerd op een tiental empirische onderzoeksvragen en het referentiemodel, zijn zes betrokken organisaties onderzocht:

- de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), met daaronder ressorterend het Nationaal Cyber Security Centrum (NCSC);
- het Defensie Computer Emergency Response Team (DefCERT);
- het Openbaar Ministerie (OM);
- de politie, in het bijzonder het Team High Tech Crime (THTC) van de Nationale Recherche;
- het computerbeveiligingsbedrijf Fox-IT.

De krijgsmacht en inlichtingendiensten, evenals de botnetintentie cyberoorlog en bestrijdingsmethoden en competenties gericht op de fysieke uitschakeling van infrastructuur of van de botmaster zelf, zijn, gezien hun specifieke taakstelling, niet verder onderzocht.

Naast genoemde organisaties spelen internetaanbieders, computerbeveiligingsbedrijven en vitale bedrijven een belangrijke rol bij de bestrijding van botnets. Gezien het grote aantal betrokken organisaties is omwille van de beschikbare tijd en middelen gekozen om het zwaartepunt bij civiele overheidsinstanties te leggen en daarnaast één prominent computerbeveiligingsbedrijf te onderzoeken. De onderzochte organisaties werken allemaal nauw samen met elkaar en met de andere betrokken partijen. Daarom kan op basis van de onderlinge consistentie van de geïnterviewden en de beschikbare secundaire bronnen de validiteit en betrouwbaarheid voldoende worden gewaarborgd, ondanks dat de ervaringen en zienswijzen van internetaanbieders en vitale bedrijven niet in dit onderzoek zijn verwerkt.

De onderzochte organisaties en de andere betrokken partijen kennen een brede samenwerking, voornamelijk voor competenties waarbij specifieke kennis van informatietechnologie en botnets nodig is. De samenwerking kenmerkt zich door multilaterale samenwerkingsverbanden in fora en werkgroepen, en de inzet van liaisonfunctionarissen. Wederzijdse belangen en wederzijds vertrouwen spelen daarin een grote rol.

Hoewel relatief eenvoudige botnets in Nederland effectief bestreden kunnen worden in de huidige opzet, wordt een aantal individuele en gezamenlijke competenties en bevoegdheden gemist om ook complexere en buitenlandse botnets aan te pakken. Ten eerste beschikt geen van de partijen over de competenties om complexere botnets te verstoren met gemanipuleerde bots of door manipulatie de communicatie over te nemen. Ten tweede is de insteek van het OM dat het terughackverbod gehandhaafd blijft en dat de overheid het alleenrecht heeft om essentiële competenties voor botnetbestrijding aan te wenden, namelijk door manipulatie van de communicatie en/of door het overnemen van een commandoserver de controle over een botnet te krijgen.

Omdat de publiek-private samenwerking hoofdzakelijk op wederzijdse belangen en wederzijds vertrouwen is gebaseerd, is het essentieel dat de overheid dat monopolie ook weet waar te maken. Anders verliest zij het vertrouwen en zien de private partijen hun belangen onvoldoende behartigd, met als gevolg dat de noodzakelijke samenwerking onder druk komt te staan. De overheid is namelijk afhankelijk van internetaanbieders, computerbeveiligingsbedrijven en vitale bedrijven, die, ondanks onvoldoende bevoegdheden voor de meest essentiële competenties, wel over (andere) belangrijke competenties voor botnetbestrijding beschikken.

Enerzijds ontbreekt dus een aantal competenties dat nodig is voor de bestrijding van complexere botnets; anderzijds kan een aantal essentiële competenties voor de bestrijding van botnets alleen door de overheid worden aangewend. Bovendien is het de vraag of de huidige noodzakelijke samenwerkingsverbanden tussen de overheid en private partijen houdbaar is voor de langere termijn. In antwoord op de hoofdvraag kan daarom worden gesteld dat de botnetbestrijding organisatorisch nog niet volledig effectief is ingericht in Nederland.

Op basis van de onderzoeksresultaten is het aan te bevelen om te onderzoeken onder welke omstandigheden een private partij ‘digitale zelfverdediging’ kan toepassen. Een andere mogelijkheid kan liggen in een door de overheid opgezet en aangestuurd structureel operationeel raamwerk voor *cyber defence* waarin gezamenlijke belangen en competenties structureel worden gewaarborgd.

Inhoudsopgave

Lijst van Tabellen en Figuren

1. Lijst van Tabellen

2. Lijst van Figuren

Voorwoord

Na mijn studie aan de Koninklijke Militaire Academie tot Officier Elektronica met een specialisatie op het gebied van interoperabiliteit van commandovoeringssystemen, wilde ik mijn kennis vanaf 2005 verder verbreden met een studie bedrijfsinformatica. Omdat ik die studie moest zien te combineren met mijn werk bij de luchtmacht, bood de master *Business Process Management and Information Technology* aan de Open Universiteit mij de beste mogelijkheden om op verschillende tijden en plaatsen te kunnen studeren.

De studie vorderde gestaag naast mijn reguliere werk. Medio 2012 voldeed ik aan de toelatingseisen voor het afstudeertraject. Vanwege mijn achtergrond en de actualiteit ging mijn interesse uit naar een onderwerp binnen het onderzoeksdomein *Security* bij de Faculteit Informatica. Tijdens de kennismaking met Harald Vranken, die mij in het afstudeertraject zou begeleiden, werd al snel duidelijk dat ik mij een jaar lang zou vastbijten in het fenomeen 'botnets'. De afstudeeropdracht richtte zich specifiek op de wijze waarop in Nederland de bestrijding van botnets is georganiseerd.

Het resultaat ligt voor u in de vorm van dit onderzoeksrapport. Ik hoop hiermee inzicht te geven hoe in Nederland de bestrijding van botnets is georganiseerd en bij te dragen aan verbetering van de bestrijding van de grootste cyberdreiging voor Nederland. Daarnaast wil ik met dit rapport het onderwerp meer inzichtelijk maken voor mensen die niet direct met deze materie te maken hebben.

Het onderzoek had niet uitgevoerd kunnen worden zonder de hulp van anderen. Ik wil Harald bedanken voor zijn constructieve terugkoppeling in alle stadia van het onderzoeksproces. Hij bood mij de ruimte om zelfstandig invulling te geven aan het onderzoek, terwijl hij mij gelijktijdig scherp hield door mijn werk regelmatig van een kritische noot of vraag te voorzien. De geïnterviewden dank ik voor de moeite die zij hebben willen nemen om mij te woord te staan. Het heeft mij niet alleen de benodigde onderzoeksgegevens opgeleverd, maar ook interessante en verhelderende gesprekken over het onderwerp. Tot slot wil ik mijn naasten bedanken voor hun steun tijdens mijn studie.

Timo Schless

September 2013

1. Inleiding

1.1. Aanleiding tot het onderzoek

Botnets zijn netwerken van geïnfecteerde computers en mobiele apparaten, zogenaamde '*bots*' die onder controle staan van iemand die er gecoördineerde aanvallen op computersystemen mee uitvoert. Het betreft bijvoorbeeld: het versturen van *spam* en *phishing* e-mails; het beïnvloeden van enquêtes, verkiezingen en markten door *click fraud*[1]; het uitvoeren van *distributed denial-of-service* (DDOS) aanvallen; het stelen van informatie, zoals wachtwoorden; of het uitvoeren van *man-in-the-middle* aanvallen. Botnets kunnen zelfs een rol spelen in een cyberaanval op een land[2]. (Li, Jiang, & Zou, 2009; Puri, 2003)

De definitie van wat een botnet precies is, is in de wetenschappelijke literatuur nagenoeg eenduidig. Hoewel de bewoordingen enigszins verschillen, beschouwen alle auteurs botnets als netwerken van schadelijke software op gehackte of geïnfecteerde computers die onder controle van een persoon of organisatie staan. Hoewel de algemene term 'botnet' neutraal zou kunnen worden opgevat als een vorm van *distributed computing*, wordt een botnet over het algemeen, en in de context van dit onderzoek, gezien als een platform waarmee ongewenste of illegale activiteiten kunnen worden uitgevoerd. Botnets worden zowel gebruikt om aanvallen uit te voeren op computers die onderdeel zijn van het botnet (interne aanval) als op computers buiten het botnet (externe aanval). (Puri, 2003; Rajab, Zarfoss, Terzis, & Monrose, 2006; *Taxonomy of Botnet Threats*, 2006; Wang, Aslam, & Zou, 2010)

Degene die controle heeft over het botnet is de *botmaster*, *botherder* of aanvaller (*attacker*). Een computer, server, mobiele telefoon, etc. die deel uitmaakt van een botnet wordt een *bot* genoemd, de software een *botagent*. Een botagent is een vorm van schadelijke software (*malware*), zoals een computervirus, waar de functionaliteiten zijn ingebouwd om de malware verder te verspreiden, om commando's van de botmaster te ontvangen en om aanvallen uit te voeren. Wanneer de schadelijke software aanwezig is op een computer, maar niet actief is in het netwerk, wordt van een *zombie* gesproken. Een computer die wordt aangevallen door een botnet is het *target*. Het target kan zelf als bot onderdeel van het botnet zijn, maar dat hoeft niet.

Liu, Xiao, Ghaboosi, Deng, & Zhang (2009) zien een botnet als een groep bots die met hulp van een commandostructuur in staat is een zelfverspreidend, zelforganiserend en autonoom raamwerk te vormen. Zelfverspreidend wil zeggen dat de botmaster niet alle computers handmatig hoeft te 'hacken' om de botagent te installeren en er een bot van te maken, maar dat het botnet mechanismen heeft om dat zelf te doen. Een botnet kan dus doorgroeien, ook als de botmaster niets doet. Met zelforganiserend en autonoom wordt bedoeld dat bots en centrale servers mechanismen hebben om zelf de onderlinge communicatie op te zetten, te onderhouden en opdrachten uit te voeren; de botmaster hoeft zich niet met de organisatie daarvan bezig te houden, en een botnet blijft dus ook intact als een botmaster (enige tijd) niets doet. In aanvulling daarop wijzen Mendonça & Santos (2012) op een ander essentieel aspect, namelijk dat de activiteiten in een botnet gecoördineerd plaatshebben.

Dit onderzoek hanteert op basis van genoemde literatuurbronnen de volgende definitie:

> *Een botnet is een zelfverspreidend en zelforganiserend gedistribueerd computerplatform dat gebruik maakt van onvrijwillig geïnfecteerde computers ('bots') in een netwerk (doorgaans het 'internet') en dat zowel intern als extern zelfstandig cyberaanvallen in opdracht van een persoon of organisatie gecoördineerd kan uitvoeren.*

De grootte van een botnet kan variëren van enkele honderden tot vele duizenden computers. Door gebruik te maken van zoveel computers blijft de eigenlijke aanvaller anoniem, terwijl hij tegelijk een groot computerpotentieel tot zijn beschikking heeft. De dreiging van botnets wordt in de literatuur als groot

[1] "FBI 'Operation Ghost Click' raid shuts down cyber criminals." (2011, November 10). *Telegraph.co.uk*. Retrieved from http://www.telegraph.co.uk/technology/news/8881382/FBI-Operation-Ghost-Click-raid-shuts-down-cyber-criminals.html

[2] "Hackers Take Down the Most Wired Country in Europe." (2007, August 21). *WIRED*. Retrieved November 20, 2012, from http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

gezien vanwege hun anonimiteit, schaalgrootte en onopgemerktheid. (J. Liu et al., 2009; Tyagi & Aghila, 2011; Vogt, Aycock, & Jacobson, 2007)

Het Cybersecuritybeeld 2013 geeft aan dat botnets een van de grootste cyberdreigingen voor Nederland vormen (*Cybersecuritybeeld Nederland 2013*, 2013). Dat is onder meer gebaseerd op het aantal besmette machines en op de schade die wordt aangericht. Hoeveel botnets er bestaan, is niet bekend, maar een onderzoek van de Technische Universiteit Delft kwam in 2011 tot een aantal van tussen de 450.000 en 900.000 geïnfecteerde computers in Nederland die over een periode van 18 maanden deel uitmaakten van een botnet (Eeten, Asghari, Bauer, & Tabatabaie, 2011). De schade die een enkel botnet al kan aanrichten, blijkt onder meer uit nader onderzoek van het Pobelka-botnet door het Nationaal Cyber Security Centrum (NCSC) in samenwerking met onder meer politie en inlichtingendiensten. Dit botnet was in staat financiële transacties tijdens het internetbankieren te manipuleren en verkreeg als bijvangst een grote hoeveelheid data van overheid, bedrijven en particulieren, zoals wachtwoorden voor e-mailservers, sociale netwerkdiensten en andere accounts (*Nadere analyse Pobelka-botnet*, 2013).

Het Ministerie van Veiligheid & Justitie geeft in de Nationale Cyber Security Strategie het belang weer van gezamenlijk (militair-civiel, publiek-privaat, nationaal-internationaal) optreden tegen cyberdreigingen als botnets om schade door misbruik, verstoring of uitval te voorkomen (Ministerie van Veiligheid & Justitie, 2011). Maar het strategisch kader maakt niet inzichtelijk over welke capaciteiten betrokken organisaties zouden moeten beschikken om effectief op te treden tegen concrete dreigingen van botnets. Daarvoor zou meer gedetailleerd moeten worden gekeken naar de eigenschappen van botnets en de onderlinge organisatie van betrokken instanties. Dit onderzoek brengt daarom in kaart of de betrokken organisaties in Nederland over de benodigde competenties en bevoegdheden beschikken om botnets te bestrijden.

1.2. Opzet van dit rapport

Het onderzoek is uitgevoerd in twee delen: een theoretisch en empirisch deel. Het theoretisch deel heeft zich gericht op het beantwoorden van theoretische onderzoeksvragen door middel van literatuuronderzoek. Het resultaat hiervan is een conceptueel model of een referentiemodel, dat als uitgangspunt heeft gediend voor de empirische toetsing. Het is uitgevoerd conform de fasering in Bijlage A.

Dit rapport is het afstudeerverslag of eindrapport van het onderzoek. Paragraaf 1.3 hieronder werkt de probleemstelling van het onderzoek nader uit. Hoofdstuk 2 bespreekt de wijze en methode waarop het onderzoek is opgezet en uitgevoerd. Hoofdstuk 3 en 4 gaan in op de theoretische en empirische onderzoeksresultaten, waarna in Hoofdstuk 5 de conclusies worden getrokken en aanbevelingen worden gedaan.

1.3. Probleemstelling

1.3.1. Doelstelling

Paragraaf 1.1 schetst kort de achtergrond van botnets en van de bestrijding ervan. De hoofddoelstelling voor dit afstudeeronderzoek is daarop gebaseerd en luidt:

> *Het doel van het onderzoek is vaststellen of de bestrijding van botnets in Nederland zodanig is georganiseerd dat daarmee de bestrijding van botnets effectief mogelijk is.*

Met ´effectief mogelijk´ wordt bedoeld dat met de huidige samenwerking van betrokken instanties alle benodigde competenties voor botnetbestrijding ook (kunnen) worden aangewend. Een ‘competentie’ wordt hier beschouwd als het vermogen waarover een groep of organisatie beschikt om een bepaald, gemeenschappelijk doel te realiseren (Weggeman, 1997). Concreet is de theoretische subdoelstelling als volgt geformuleerd:

> *Het theoretisch deel van het onderzoek heeft tot doel een model vast te stellen dat weergeeft welke soorten partijen met welke competenties en bevoegdheden nodig zijn bij de bestrijding van botnets.*

Het empirisch deel van het onderzoek heeft vervolgens tot doel te toetsen of het referentiemodel compleet en correct is. Met andere woorden: komt het model overeen met de wijze waarop in Nederland de botnetbestrijding is georganiseerd.

> *Het empirisch deel van het onderzoek heeft tot doel te toetsen of het referentiemodel – dat op basis van noodzakelijke competenties en bevoegdheden weergeeft welke partijen er betrokken zijn bij de bestrijding van botnets – overeenkomt met de wijze waarop in Nederland de botnetbestrijding is georganiseerd.*

Aan de hand van de uitkomsten van het empirisch deel kunnen de verschillen tussen het model en de werkelijkheid worden geanalyseerd en verklaard.

1.3.2. **Vraagstelling**

Uit de hoofddoelstelling volgt de hoofdvraag van het onderzoek:

> *Is de bestrijding van botnets organisatorisch effectief ingericht in Nederland?*

Het theoretisch deel van het onderzoek is uitgevoerd aan de hand van de volgende vier onderzoeksvragen.

[T.1] *Welke soorten botnets kunnen op basis van hun eigenschappen worden onderscheiden?*

Deze vraag vormt de rode draad in Paragraaf 3.1 van dit rapport en leidt tot een taxonomie voor botnets. Om de onderzoeksvraag te beantwoorden, is gebruik gemaakt van een aantal subvragen:

1. Wat is een botnet?
2. Wat zijn typische kenmerken van een botnet?
3. Welke van die kenmerken zijn bruikbaar om een indeling van soorten botnets te maken?

[T.2] *Welke methoden kunnen worden onderscheiden voor de bestrijding van botnets?*

Deze onderzoeksvraag komt aan bod in Paragraaf 3.3. Om deze onderzoeksvraag te beantwoorden is gebruik gemaakt van een aantal subvragen:

1. Hoe kan een botnet worden ontdekt of opgespoord?
2. Hoe kunnen structuur en bouw van een specifiek botnet in kaart worden gebracht?
3. Hoe kan de de botmaster worden opgespoord?
4. Hoe kan een botnet met een bepaalde structuur worden bestreden of uitgeschakeld?

[T.3] *Welke competenties en bevoegdheden zijn nodig voor de toepassing van de geïdentificeerde bestrijdingsmethoden [T.2]?*

[T.4] *Welke soorten organisaties zouden betrokken moeten zijn bij een effectieve bestrijding van botnets, gegeven de geïdentificeerde benodigde competenties en bevoegdheden [T.3]?*

Paragraaf 3.4 behandelt deze twee onderzoeksvragen. Om deze onderzoeksvragen te beantwoorden is gebruik gemaakt van een aantal subvragen, waarbij primair wordt uitgegaan van de Nederlandse situatie:

1. Welke competenties zijn nodig voor de bestrijding van botnets?
2. Welke (soort) organisaties zijn betrokken bij de bestrijding van botnets?
3. Over welke bevoegdheden beschikken die organisaties?
4. Welke competenties en bevoegdheden uit onderzoeksvraag [T.3] zijn daarmee afgedekt?

Op basis van de onderzoeksresultaten wordt in Paragraaf 3.6 het referentiemodel voor botnetbestrijding beschreven dat als uitgangspunt dient voor toetsing aan de hand van de volgende empirische onderzoeksvragen.

Het empirisch deel van het onderzoek is uitgevoerd aan de hand van de volgende tien onderzoeksvragen, waarin eerst wordt nagegaan welke concrete organisaties in Nederland aan botnetbestrijding doen.

[E.1] *Welke Nederlandse organisaties bestrijden botnets?*

Deze vraag komt aan bod in Paragraaf 4.3.1.

Om te bepalen in hoeverre men in de praktijk op eenzelfde wijze als in de literatuur naar botnetbestrijding kijkt, wordt in Paragrafen 4.3.2 tot en met 4.3.5 gekeken welke botnettaxonomie en -bestrijdingsmethoden door betreffende organisaties worden gehanteerd en hoe de competenties en bevoegdheden zijn georganiseerd of verdeeld:

[E.2] *Hanteren de organisaties van [E.1] de onder [T.1] en [T.2] geïdentificeerde of vergelijkbare botnettaxonomie en –bestrijdingsmethoden, of hanteren zij een andere benadering?*

[E.3] *Op welke wijze zijn de organisaties voor de bestrijding van botnets georganiseerd?*

[E.4] *Over welke bevoegdheden en competenties beschikken de organisaties uit onderzoeksvraag [E.1] en wanneer worden die aangewend?*

[E.5] *Voor welke competenties en bevoegdheden werken de betrokken organisaties [E.1] samen met andere organisaties?*

De gegevens van de eerste drie empirische onderzoeksvragen worden vervolgens met behulp van het referentiemodel geanalyseerd aan de hand van de volgende vragen:

[E.6] *Dekken de Nederlandse organisaties alle aspecten van botnetbestrijding uit het referentiemodel af?*

[E.7] *Welke competenties en bevoegdheden [T.3] hebben en gebruiken de organisaties [E.1], individueel of gezamenlijk, en welke niet?*

[E.8] *Welke geïdentificeerde bestrijdingsmethoden [T.2] worden in de praktijk gebracht, en welke niet?*

[E.9] *Bestaan er daardoor geïdentificeerde soorten botnets [T.1] die niet kunnen worden bestreden?*

Tot slot brengt het empirisch deel de afwijkingen tussen het referentiemodel en de werkelijkheid in kaart.

[E.10] *Welke verschillen kunnen worden vastgesteld tussen de wijze waarop de bestrijding van botnets in Nederland is georganiseerd en het referentiemodel voor botnetbestrijding?*

Hiermee kan in Hoofdstuk 5 de hoofdvraag of de bestrijding van botnets organisatorisch effectief is ingericht in Nederland, worden beantwoord en kunnen conclusies worden getrokken.

2. Onderzoeksopzet

2.1. Object van Onderzoek

2.1.1. Afbakening

Het onderzoek richt zich op de organisatie van botnetbestrijding in Nederland. Voor het opstellen van het referentiemodel in het theoretisch deel heeft het onderzoek zich echter niet uitsluitend tot Nederland beperkt om tot een zo algemeen mogelijk model te komen.

Hoewel de bestrijding niet los te zien is van bescherming tegen botnets, laat het onderzoek de bescherming (i.e. het nemen van preventieve maatregelen) buiten beschouwing.

Het onderzoek tracht het hele veld van de organisatie van botnetbestrijding in kaart brengen. Gezien de grootte en complexiteit van het onderwerp, zijn de diepgang en het detailniveau beperkt gehouden.

2.1.2. Onderzoekspopulatie

De onderzoekspopulatie bestaat uit Nederlandse publieke en private organisaties. In het theoretisch deel worden deze organisaties algemeen besproken. In het empirisch deel is een selectie van specifieke organisaties onderzocht; de selectie wordt in Paragraaf 2.5.2 nader toegelicht.

2.2. Onderzoeksbenadering en -strategie

Het onderzoek is verkennend van aard. Volgens Saunders et al. (2011) zijn de belangrijkste manieren om een verkennend onderzoek uit te voeren een literatuuronderzoek en interviews met experts of focusgroepen. In lijn hiermee bestaat het theoretisch deel van het onderzoek uit een literatuurstudie en het empirisch deel uit interviews. De nadruk ligt op het verkrijgen van een gegeneraliseerd inzicht in de organisatie van botnetbestrijding en de aspecten die daarbij een rol spelen op basis van een gelimiteerde hoeveelheid beschikbare kennis over botnets.

Het theoretisch deel heeft primair een inductieve opzet. Van belang bij het literatuuronderzoek is het creëren van een goed begrip van de onderzoekscontext en het zo gestructureerd mogelijk vastleggen van de kwalitatieve onderzoeksgegevens in een referentiemodel als basis voor verder empirisch onderzoek.

De empirische onderzoeksbenadering legt de nadruk op het vergelijken van het referentiemodel met de werkelijkheid. Het empirisch deel operationaliseert de concepten zoveel mogelijk en verzamelt de gegevens om de modellen met de werkelijkheid te vergelijken en de verschillen daartussen te verklaren. Er is dus sprake van een meer deductieve benadering waarbij wordt gekeken of de conclusies die getrokken kunnen worden op basis van het referentiemodel ook empirisch gezien houdbaar zijn.

2.3. Methode van onderzoek voor het theoretisch deel

Het theoretisch onderzoeksdeel is uitgevoerd door middel van literatuuronderzoek. Op basis van de methoden van Saunders et al. (2011) en Levy & Ellis (2006), worden per theoretische onderzoeksvraag de volgende stappen in een iteratief proces doorlopen:

1. Zoeken van literatuur op basis van tertiaire bronnen, internet en bronverwijzingen in eerder gevonden primaire en secundaire literatuur;
2. Beoordelen en structureren van de gevonden literatuur op basis van kwaliteit en relevantie;
3. Vastleggen van bibliografische gegevens;
4. Gebruik van informatie uit de bron om de theoretische onderzoeksvragen te beantwoorden.

Bij het zoeken naar literatuur is voornamelijk gebruik gemaakt van de zoekfuncties van de Open Universiteit, ACM Digital Library, IEEE Digital Library en Google Scholar. De onderzoeksvragen en afgeleide subvragen maken het mogelijk gericht te zoeken vanuit de concepten en sleutelwoorden. Dat geeft richting

aan het identificeren van relevante literatuur (pt.1) en aan het structureren ervan (pt.2). Daarbij is gebruik gemaakt van de Zotero research tool[3] om de literatuur op te slaan, te structureren, te indexeren en bibliografische gegevens vast te leggen (pt.3).

Op basis van titel en samenvatting zijn 100 artikelen gescand om te zien welke het beste aansloten bij de onderzoeksvragen en subvragen (pt.4). Daarnaast zijn 15 artikelen als referentie van een andere bron opgezocht. De kwaliteit en relevantie van de geselecteerde literatuurbronnen volgde uit de mate waarin de bron antwoord geeft op de onderzoeksvraag of subvraag. Maar ook de ouderdom van de bron, de mate waarin de bron is gebaseerd op andere (relevante) bronnen, en de mate waarin de bron in lijn of juist in tegenspraak is met andere literatuur vormden belangrijke selectiecriteria.

Bijlage C bevat een nadere toelichting op de uitgevoerde literatuurselectie.

2.4. Methode van onderzoek van het empirisch deel

In dit onderzoek bestaat de populatie niet zozeer uit individuele personen maar uit organisaties. Daarom is in lijn met de onderzoeksstrategie een casestudy in de vorm van een semigestructureerd of kwalitatief onderzoeksinterview uitgevoerd. Het interview is gehouden met vertegenwoordigers en/of experts die namens de te onderzoeken publieke en private organisaties kunnen spreken over de aspecten uit het conceptueel model. Gezien de complexiteit van de materie en het abstractieniveau van het onderzoek is een semigestructureerd interview het meest geschikt, omdat het de interviewer in staat stelt de vragen toe te lichten en om door te vragen.

Bij het interview is gebruik gemaakt van gestandaardiseerde vragen, zodat het interview consistent is met de doelstelling en onderzoeksvragen van het empirisch deel. De empirische onderzoeksvragen vormen hiervoor met het referentiemodel de basis om de vertegenwoordigers en/of experts van de geselecteerde organisaties zo gestructureerd mogelijk te interviewen. Het interview doorloopt zo aan de hand van de onderzoeksvragen op systematische wijze het referentiemodel.

Er bestond daarbij een risico dat de empirische gegevens dermate afwijken dat ze niet in de structuur van het referentiemodel zouden passen, wat een inhoudelijke vergelijking moeilijk of onmogelijk maakt. In dat geval zou de onderzoeksmethode moeten worden aangepast. In plaats van een deductieve insteek, zou dan voor een inductieve insteek zijn gekozen om tot een alternatieve generalisatie te komen. Dit is echter niet nodig gebleken.

Een alternatief voor een verkennend onderzoek zou een meervoudige casestudy zijn geweest, waarin wordt bestudeerd hoe het verloop van de bestrijding van verschillende botnets is aangepakt door betrokken organisaties. Maar dan was de kans groot dat, gezien de vele verschijningsvormen van botnets, niet alle aspecten van het referentiemodel aan bod komen. Daarnaast zou een dergelijke casestudy in grote mate afhankelijk zijn van de beschikbaarheid en toegankelijkheid van de informatie bij een aantal betrokken organisaties. Onderzoekstrategieën als een experiment en action research zijn voor dit verkennend onderzoek ongeschikt en praktisch niet uitvoerbaar om samenwerking tussen organisaties te onderzoeken gezien de grootte van het speelveld en de beschikbare tijd.

2.5. Uitvoering van het onderzoek

2.5.1. Operationalisering

De literatuurstudie geeft in het conceptueel model weer welke aspecten voor het onderzoek deel uitmaken van de organisatie van botnetbestrijding. Met het uitwerken van het referentiemodel zijn de conceptuele aspecten (intentie en structuur van het botnet, bestrijdingsmethoden, competenties en bevoegdheden) reeds concreet gemaakt. Op basis van de empirische onderzoeksvragen en het referentiemodel zijn vervolgens gestructureerde onderzoeksvragen gemaakt. De interviewvragen zijn opgenomen in Bijlage E.

[3] Zie https://www.zotero.org/. De bibliografische database is beschikbaar in BibTeX, BibIX, Dublin Core RDF format.

2.5.2. **Onderzoekspopulatie en -selectie**

De onderzoekspopulatie bestaat uit Nederlandse publieke en private organisaties die betrokken zijn bij de bestrijding van botnets. Onderzoeksvraag [E.1] is bedoeld om die organisaties in kaart te brengen. Tegelijkertijd moest er een selectie binnen die populatie worden gemaakt, omdat het praktisch onmogelijk is alle organisaties individueel te onderzoeken. De nadruk ligt op de publieke organisaties.

2.5.3. **Selectie van te onderzoeken organisaties**

Het literatuuronderzoek heeft de volgende Nederlandse publieke organisaties geïdentificeerd die een (mogelijke) rol spelen bij botnetbestrijding:

- de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), in het bijzonder het Nationaal Cyber Security Centrum (NCSC);
- de Algemene Inlichtingen- en Veiligheidsdienst (AIVD);
- de krijgsmacht, waaronder de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Koninklijke Marechaussee (KMAR);
- het Openbaar Ministerie (OM);
- de politie, in het bijzonder het Team High Tech Crime (THTC) van de Nationale Recherche.

In het literatuuronderzoek werden geen specifieke private organisaties aangeduid die een belangrijke rol spelen bij botnetbestrijding; er worden soorten organisaties aangeduid waarvan internetaanbieders, computerbeveiligingsbedrijven en vitale bedrijven de belangrijkste spelers voor botnetbestrijding zijn. Gezien het grote aantal van deze organisaties in Nederland is er voor het onderzoek een selectie gemaakt. Omwille van de beschikbare tijd en middelen is ervoor gekozen om het zwaartepunt bij civiele overheidsinstanties te leggen en daarnaast één prominent computerbeveiligingsbedrijf te onderzoeken, te weten Fox-IT. Computerbeveiligingsbedrijven werken in principe voor andere organisaties en kunnen vanuit die positie een breed beeld geven hoe zij botnetbestrijding bij hun klanten, met name internetaanbieders en vitale bedrijven, inrichten en hoe de private sector samenwerkt met de publieke sector.

Ieder van deze organisaties werd aangeschreven met het verzoek één of meer functionarissen te interviewen die inzicht kunnen geven in de competenties en bevoegdheden van de organisaties voor de bestrijding van botnets.

Gezien de terughoudende respons van de krijgsmacht en de inlichtingendiensten, hun eigen bijzondere taakstelling en beperkte interactie met andere organisaties, is besloten deze verder buiten het empirisch deel van het onderzoek te laten. Uit geen van de afgenomen interviews blijkt dat de krijgsmacht momenteel voor andere partijen een cruciale rol op het gebied van botnetbestrijding vervult.

2.5.4. **Validiteit**

De validiteit van het onderzoek is de mate waarin daadwerkelijk is gemeten wat beoogd werd te meten, zodat de juiste conclusies kunnen worden getrokken. Gezien de betrekkelijk eenvoudige onderzoeksmethode en operationalisering, is het afbreukrisico voor de validiteit van dit onderzoek beperkt. In het literatuuronderzoek is met voorbeelden beschreven wat er onder de verschillende aspecten van botnetbestrijding moet worden verstaan.

De interviewmethode heeft de onderzoeker in staat gesteld tijdens het interview door te vragen wat de geïnterviewde bedoelde om zeker te stellen dat beweringen betrekking hadden op de juiste aspecten van het referentiemodel.

Verder is niet aannemelijk dat dit onderzoek zelf het onderzoeksobject, nl. de organisatie van botnetbestrijding in Nederland, heeft beïnvloed. De bevoegdheden en competenties van de te onderzoeken organisaties zijn gedurende het onderzoek niet significant veranderd.

2.5.5. **Betrouwbaarheid**

De betrouwbaarheid van het onderzoek is de mate van onafhankelijkheid van het toeval. Belangrijke criteria hiervoor zijn: de consistentie van gegevens en uitsluiting van het toeval. Gezien de hoge mate van structuur

in het referentiemodel dat op extern onderzoek is gebaseerd, en de strikte samenhang tussen het referentiemodel, de empirische onderzoeksvragen en de interviewvragen, is het voldoende aannemelijk dat het empirisch onderzoek bij herhaling of met een andere waarnemer gelijke resultaten zal geven.

Deelnemersfouten en -vertekening zijn met een interviewstrategie zoveel mogelijk voorkomen. Enerzijds is er op aangestuurd een of meer personen te interviewen die gezien hun functie binnen de organisatie de meest aangewezen functionarissen zijn om antwoord te kunnen geven op de interviewvragen. Anderzijds is in het interview kritisch doorgevraagd om 'politiek correcte' en subjectieve antwoorden te voorkomen en om eenduidige antwoorden te krijgen. De gestructureerdheid van de interviewvragen heeft daar ook aan bijgedragen.

Het beperkte aantal onderzochte organisatie doet in beginsel afbreuk aan de betrouwbaarheid van het interview. Gezien de specifieke rol van de onderzochte organisaties is dit echter beperkt oplosbaar. Daarom is getracht de betrouwbaarheid te vergroten door aan iedere organisatie expliciet te vragen naar de bevoegdheden en competenties die andere organisaties (zouden moeten) hebben. Per organisatie zijn dus niet alleen gegevens van die organisatie zelf, maar ook van de daarmee samenwerkende organisaties verzameld.

De keuze om in de private sector slechts één computerbeveiligingsbedrijf te onderzoeken, doet echter wel afbreuk aan de betrouwbaarheid van onderzoeksgegevens over de botnetbestrijding door internetaanbieders en vitale bedrijven. Op basis van consistentie met andere geïnterviewden en beschikbare secundaire bronnen kan worden gesteld dat het algemene beeld van andere betrokken organisaties houdbaar is, maar dat neemt niet weg dat de ervaringen en zienswijzen van voornamelijk internetaanbieders en vitale bedrijven in verschillende sectoren niet in dit onderzoek zijn verwerkt.

Tot slot hebben de geïnterviewden de interviews nagelezen en goedgekeurd om de validiteit (staat er wat men bedoelde te zeggen) en betrouwbaarheid van de empirische onderzoeksgegevens (zijn de gegevens uit het interview consistent en correct) te controleren.

3. Uitkomsten van het literatuuronderzoek naar botnetbestrijding

3.1. Introductie

Dit hoofdstuk bevat de uitkomsten van het literatuuronderzoek. Deze paragraaf gaat in op welke soorten botnets op basis van hun eigenschappen kunnen worden onderscheiden (onderzoeksvraag [T.1]). De definitie van een botnet in Paragraaf 1.1 vormt het beginpunt om kenmerken van botnets systematisch te beschouwen. In onderstaande paragrafen wordt ingegaan op de volgende elementen uit de definitie: 1. het doel dat een botnet dient voor de botmaster of voor derden; 2. de aansturing en organisatie van botnets; en 3. de infectie van computers en de verspreiding van botnets. Hiermee wordt eigenlijk een grove omgekeerde levenscyclus van een botnet beschreven: van het doel dat het botnet heeft terug naar hoe het botnet tot stand komt.

In paragraaf 3.2 wordt geëvalueerd welke eigenschappen van botnets relevant en bruikbaar zijn voor een indeling in het kader van dit onderzoek naar de organisatie voor botnetbestrijding. Dat vormt het uitgangspunt voor het identificeren van bestrijdingsmethoden in Paragraaf 3.3 aan de hand van onderzoeksvraag [T.2]. De benodigde competenties en bevoegdheden, evenals organisaties die zijn betrokken bij de bestrijding van botnets (onderzoeksvragen [T.3] en [T.4]), komen aan de orde in Paragraaf 3.4.

3.2. Eigenschappen van botnets

3.2.1. Doel van botnets

Kenmerkend voor botnets is dat ze door één of meer botmasters worden gebruik met het doel een computer- of cyberaanval (*cyber attack*) uit te voeren om een beoogd effect te bereiken (Paxton, Ahn, & Shehab, 2011).

3.2.1.1. Oogmerk en motieven voor botnetaanvallen

Zowel Tettero & de Graaf (2010) als het Nationaal Cyber Security Centrum (*Cybersecuritybeeld Nederland 2013*, 2013) presenteren een indeling van cyberaanvallen naar het motief van de aanvaller. Op basis van beide indelingen wordt in dit onderzoek de volgende indeling naar intentie of oogmerk van cyberaanvallen gehanteerd. Daarbij dient te worden vermeld dat deze motieven niet noodzakelijk het oogmerk van de botmaster zelf hoeven te zijn, omdat de botmaster zijn diensten kan hebben aangeboden aan derden.

Tabel 1. Oogmerk en motieven voor botnetaanvallen

A.	cybervandalisme (*cyber vandalism*): ongewenste maar niet noodzakelijk strafbare activiteiten, zoals het beledigen via tweets of comments, pesten via social media, etc. door individuen voor genot of als recalcitrantie.
B.	misdaad via internet[4]: strafbare activiteiten die worden ondersteund door internet, zoals kinderporno, racisme, stalking, piraterij door individuen of criminelen voor gewin of genot.
C.	cybercriminaliteit[4] (*cyber crime*): strafbare activiteiten die primair over/door internet plaatshebben, zoals *phising*, *denial-of-service* aanvallen, versturen van *spam*, beïnvloeding van enquêtes, verkiezingen en markten door *click fraud*, digitale inbraak en stelen van informatie, auteursrechtenschending met winstoogmerk, industriële spionage, etc. door criminele organisaties voor geldelijk of ander gewin.

[4] Stol, Leukfeldt & Klap (2012) zien ook een verschil tussen klassieke delicten met een digitale dimensie en cybercrime, maar ze beschouwen beide toch als één vorm van politiewerk in een digitale samenleving. Omdat hier vooral een spectrum van intenties van cyberaanvallen wordt weergegeven, zijn beide toch apart opgenomen.

D.	hacktivisme[5,6] (*hacktivism*): (dreiging met) *denial-of-service* aanvallen, digitale inbraak etc., doorgaans voor publiciteit door groeperingen met een politiek of ideologisch doel.
E.	cyberterrorisme (*cyber terrorism*): (dreiging met) sabotage van vitale voorzieningen door of namens groeperingen met een politiek of ideologisch doel.
F.	cyberoorlog[7] (*cyber warfare*, *cyber defence*): digitale spionage, (dreiging met) sabotage van vitale of militaire voorzieningen met cyberaanvallen op computersystemen, ondersteuning psychologische oorlogsvoering met spam, afdwingen censuur door of namens nationale staten.

Deze indeling is niet specifiek alleen voor botnets, maar een bepaald botnet is in principe wel te classificeren in één of meer van deze categorieën. Ook kan een botnet meer dan één botmaster hebben, die het tegelijk voor verschillende doelen gebruiken (Paxton et al., 2011). De scheidslijn tussen dadergroepen in het digitale domein is ook niet altijd duidelijk: het is bijvoorbeeld bekend dat inlichtingendiensten criminelen gebruiken voor cyberspionage (Prins, 2012).

3.2.1.2. Aanvalsvormen van botnets

Tyagi & Aghila (2011) en Liu et al. (2009) geven een overzicht van aanvalsvormen waarvan bekend is dat die door botnets worden gebruikt, evenals een uitgebreid overzicht van bekende botnets en hun aanvalsvormen.

Chapman, Leblanc & Partington (2011) beschrijven een indeling van cyberaanvallen naar de gebruikte techniek op basis van de toegangsrechten die de aanvaller heeft op het aan te vallen systeem: cyberaanvallen zonder toegang tot de systemen die (van afstand) worden aangevallen (*no access*), met beperkte toegang op gebruikersniveau (*user access*) en met volledige toegang op administratorniveau (*root access*). Onderstaande tabellen geven de belangrijkste aanvalsvormen weer gebaseerd op beschreven voorbeelden. De beschreven aanvalsvormen hoeven niet uniek voor botnets te zijn en ook andere vormen zijn niet uitgesloten[8].

Tabel 2 geeft een overzicht van aanvallen door een botnet op niet-geïnfecteerde computers, ofwel aanvallen van buitenaf waarbij geen toegang (*no access*) tot het *target* bestaat.

[5] Hoewel 'hacktivisme' bij Tettero & De Graaf niet als aparte verschijningsvorm voorkomt, is dit hier opgenomen omdat recente gebeurtenissen rond het hackerscollectief Anonymous of rond Wikileaks hebben laten zien dat er cyberaanvallen bestaan die weliswaar een politiek of ideologisch motief hebben, maar niet noodzakelijk als terroristisch zijn te bestempelen:

- "Anonymous neemt wraak voor Megaupload – 'grootste aanval ooit'". (2012, January 19). Nrc.nl. Retrieved November 19, 2012, from http://www.nrc.nl/nieuws/2012/01/19/anonymous-neemt-wraak-voor-neerhalen-megaupload/
- "Anonymous pakt opnieuw Amerikaanse overheidssites aan om ACTA." (2012, February 17). *Nrc.nl*. Retrieved November 19, 2012, from http://www.nrc.nl/nieuws/2012/02/17/anonymous-pakt-opnieuw-amerikaanse-overheidssites-aan/

[6] Merk op dat er een verschil is tussen hacktivisme en cyberactivisme; cyberactivisme heeft weliswaar ook een politiek of ideologisch doel, maar maakt niet noodzakelijk gebruik van cyberaanvallen of andere ongewenste of illegale activiteiten.

[7] De term 'cyberoorlog' is onderwerp van veel discussie. In lijn met Lodder & Boer (2012) wordt cyberoorlog hier niet gezien als een "onzichtbare oorlog op internet" waarover het nodige scepticisme bestaat, maar als cyberactiviteiten gericht tegen staten die onmiskenbaar structureel plaatshebben, en waarop niet zozeer het strafrecht maar het volkenrecht van toepassing is.

[8] Het is bijvoorbeeld bekend dat bots ook gebruik maken van zwaktes in andere software of openingen achtergelaten door eerdere virussen (Zhu et al., 2008).

Tabel 2. Aanvalsvormen van botnets op niet-geïnfecteerde computers van afstand

Aanvalsvorm	Beschrijving	Mogelijk oogmerk
verspreiding van het botnet	Zie Paragraaf 3.2.3	Kenmerkend voor alle botnets, dus past bij elk mogelijk oogmerk
distributed denial-of-service attack	Het onbruikbaar of onbereikbaar maken van computers, netwerken en daarvan afhankelijke apparatuur door het sturen van een overvloed aan netwerkverkeer (Chapman et al., 2011)(Tyagi & Aghila, 2011)(J. Liu et al., 2009)	cybervandalisme (A), cybercriminaliteit (C), hacktivisme (D), cyberterrorisme (E) en cyberoorlog (F)
spam	Verzenden van (massale) e-mails voor commerciële doeleinden, om schadelijke software te verspreiden, (Chapman et al., 2011)(Tyagi & Aghila, 2011)(J. Liu et al., 2009) of mogelijk misleidende informatie en propaganda in het kader van hacktivisme, cyberterrorisme en cyberoorlog	cybercriminaliteit (C), mogelijk ook (gerichter) in het kader van hacktivisme (D), cyberterrorisme (E) en cyberoorlog (F)
phishing / identity fraud	Verzenden van (massale) e-mails voor oplichting of het ontfutselen van informatie (Chapman et al., 2011)(Tyagi & Aghila, 2011)(J. Liu et al., 2009)	cybercriminaliteit (C), mogelijk ook (gerichter) in het kader van hacktivisme (D), cyberterrorisme (E) en cyberoorlog (F)
click fraud	beïnvloeden enquêtes, verkiezingen en advertentieverwijzingen (zgn. *click through rates*). (Tyagi & Aghila, 2011)(J. Liu et al., 2009)	cybercriminaliteit (C), mogelijk ook cybervandalisme (A) of hacktivisme (D)

Naast aanvalsvormen van botnets op niet-geïnfecteerde targets, zijn botnets in staat aanvallen uit te voeren op computersystemen die onder controle van het botnet staan, namelijk de bots zelf waarop in ieder geval *user access* en wellicht *root access* is verkregen. Hiervan geeft Tabel 3 een overzicht.

Tabel 3. Aanvalsvormen van botnets op geïnfecteerde computers, de bots zelf

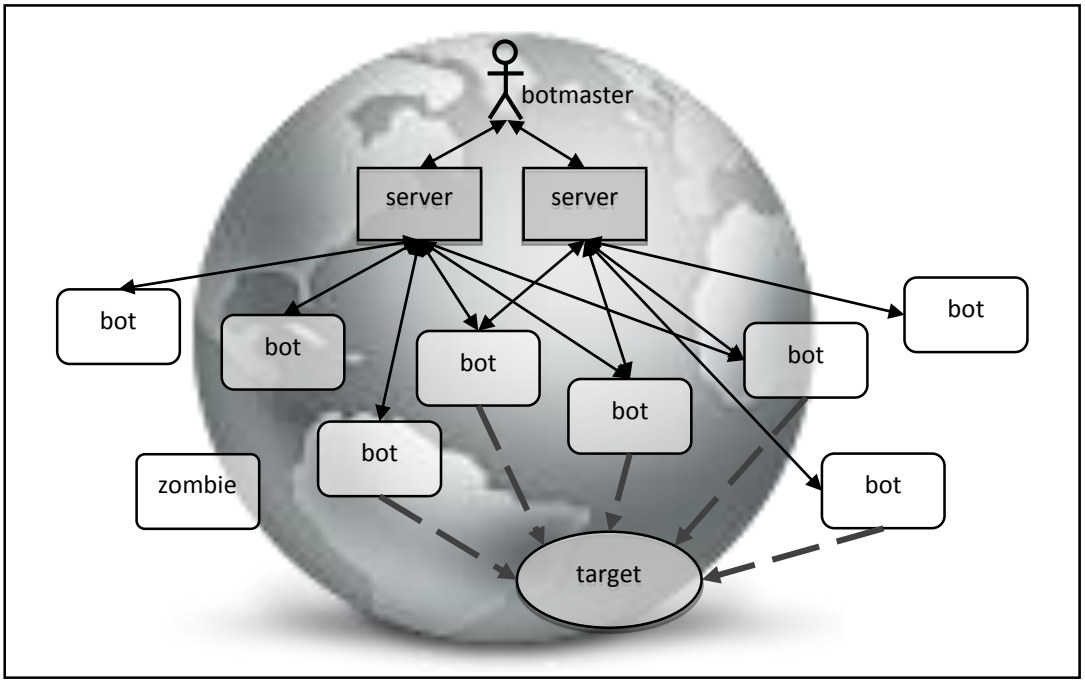
Aanvalsvorm	Beschrijving	Mogelijk oogmerk
downloaden en installeren van schadelijke software	Het installeren van aanvullende of bijgewerkte schadelijke software door de bot agent voor aanvullende of verbeterde functionaliteit. (Chapman et al., 2011)(Tyagi & Aghila, 2011)	cybervandalisme (A), cybercriminaliteit (C), hacktivisme (D), cyberterrorisme (E) en cyberoorlog (F)
sniffing	Het bekijken van netwerkverkeer om informatie zoals wachtwoorden, identiteitsgegevens of andere gevoelige informatie te achterhalen. (Chapman et al., 2011)(Tyagi & Aghila, 2011)	cybercriminaliteit (C), cyberterrorisme (E) en cyberoorlog (F)
spyware / key logging	Het registreren van toetsaanslagen om informatie zoals wachtwoorden, identiteitsgegevens of andere gevoelige informatie te achterhalen. (Chapman et al., 2011)(Tyagi & Aghila, 2011)	cybercriminaliteit (C), cyberterrorisme (E) en cyberoorlog (F)
adware	Het weergeven van ongewenste advertenties (Chapman et al., 2011)(Tyagi & Aghila, 2011)	cybercriminaliteit (C)
nuisance attacks	Het uitvoeren van hinderlijke activiteiten op computersystemen (Chapman et al., 2011)	cybervandalisme (A), hacktivisme (D) en cyberoorlog (F)
logic bombs / ransomware	Het (dreigen met) uitschakelen van computersystemen of wissen van gegevens als niet aan bepaalde voorwaarden wordt voldaan. (Chapman et al., 2011)	cybercriminaliteit (C), cyberterrorisme (E) en cyberoorlog (F)
opslaan van verboden gegevens	De geïnfecteerde computer wordt gebruikt om verboden gegevens op te slaan (Puri, 2003)	misdaad over internet (B), cybercriminaliteit (C)

3.2.2. **Aansturing en organisatie van botnets**

Uit de definitie volgt dat botnets zelfstandig opdrachten van iemand kunnen uitvoeren; een botnet heeft dus intrinsieke eigenschappen die dat mogelijk maken, namelijk zogenaamde *command & control*[9] kanalen. De wijze waarop de commandovoering over een botnet is ingericht, is bepalend voor de structuur en de organisatie van het botnet. In de literatuur worden drie hoofdvormen van een commandostructuur besproken: centrale, decentrale en complexe hybride commandostructuren[10].

3.2.2.1. Centrale commandostructuur

Botnets met een gecentraliseerde commandostructuur maken gebruik van één of meer centrale servers die de botnets aansturen. Hierbij worden hoofdzakelijk het IRC-protocol (Internet Relay Chat) of HTTP (Hyper-Text Transfer Protocol) gebruikt om vanaf de centrale server individuele bots aan te sturen (J. Liu et al., 2009) (Patil & Kumar, 2011). De servers kunnen bestaande chat servers, blogs of twitteraccounts zijn, maar er zijn ook botnets bekend die gebruik maken van *instant messaging* (IM) diensten zoals AOL, MSN en ICQ of van een eigen protocol (Tyagi & Aghila, 2011).



Figuur 1. Schematische weergave van een botnet met centrale commandostructuur

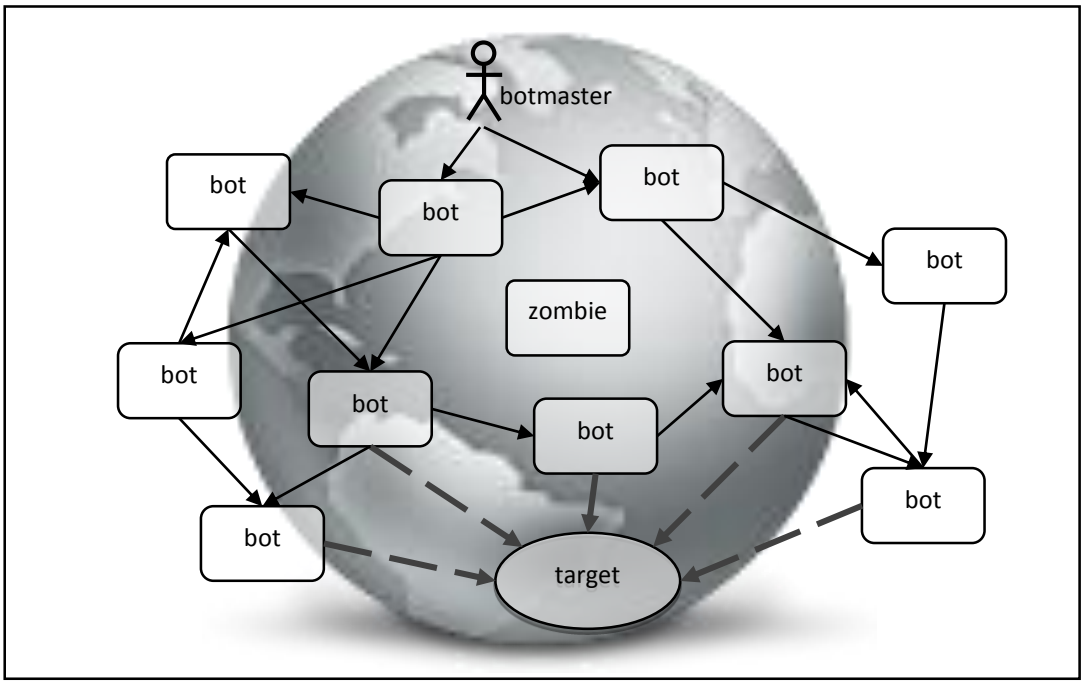
De commandolijnen van IRC- en HTTP-botnets zijn bidirectioneel, zodat de botmaster zowel commando's aan de bots kan geven als gegevens over de bot, zijn host en het gehele botnet kan verkrijgen (Xiang, Binxing, Peng, & Chaoge, 2012). Het voordeel van deze commandostructuur is het gemak waarmee de botmaster de bots kan bereiken, gegevens ervan kan opvragen en zo het hele botnet kan aansturen. De zwakte van deze structuur is de afhankelijkheid van een beperkt aantal centrale servers; als die worden overgenomen of uitgeschakeld dan is de botmaster de controle over het botnet kwijt.

[9] De Engelse term *Command & Control* is een militair begrip. De Nederlandse term is 'commandovoering'. In dit onderzoek worden de termen 'commandostructuur' en 'commandolijnen' gebruikt.

[10] Een gedetailleerde technische beschrijving van botnetcommandostructuren en protocollen valt buiten het bereik van dit onderzoek; hiervoor wordt naar de literatuur verwezen.

3.2.2.2. Decentrale commandostructuur

In een decentraal botnetmodel worden de commandolijnen opgezet door de individuele bots onderling, waardoor het botnet niet afhankelijk is van een beperkt aantal centrale servers. Dit wordt doorgaans een peer-to-peer (P2P) botnet genoemd. De botmaster geeft zijn commando's direct aan een aantal bots, die het op hun beurt verder verspreiden.



Figuur 2. Schematische weergave van een botnet met decentrale commandostructuur

Een P2P-botnet is veel robuuster dan een botnet met een centrale commandostructuur omdat het niet afhankelijk is van enkele centrale entiteiten. Daar staat tegenover dat een decentrale commandostructuur complexer en daardoor moeilijker te realiseren is. Net als bij andere P2P netwerken, kan een botnet met een decentrale commandostructuur gestructureerd of ongestructureerd van aard zijn. Een gestructureerd botnet maakt gebruik van een mechanisme, zoals een *distributed hash table*, om te bepalen welke bots verbinding maken met welke andere bots. Een ongestructureerd botnet doet dat niet en probeert willekeurig andere bots te zoeken om verbinding te maken (Wang, Aslam, et al., 2010).

Voor een P2P-botnet is het lastig om een commando voor alle bots tegelijk te geven, omdat de propagatietijd onzeker is. De commandokanalen zijn doorgaans unidirectioneel (Xiang et al., 2012) waardoor het voor een botmaster moeilijker is informatie van individuele bots en over het hele botnet te verkrijgen. Bovendien moet de botmaster zorgen dat individuele bots niet zomaar commando's van anderen accepteren door bijvoorbeeld authenticatie en encryptie toe te passen (Tyagi & Aghila, 2011).

3.2.2.3. Hybride commandostructuur en flux netwerken

Recent onderzoek laat zien dat botnets complexer worden door gebruik te maken van gecombineerde technieken om met de sterke punten van één techniek de zwakke punten van de andere techniek te compenseren.

Wang, Sparks, & Zou (2010) laten zien dat een hybride vorm tussen een centrale en decentrale commandostructuur een botnet moeilijk te ontdekken en zeer robuust maakt. In plaats van enkele centrale servers, maakt het botnet gebruik van een decentraal netwerk van '*bot servants*'. Dat zijn bots die niet alleen commando's uitvoeren maar ook commando's in het botnet aan andere bots doorgeven. (Wang, Sparks, et al., 2010) (Lu, Liao, & Chen, 2011)

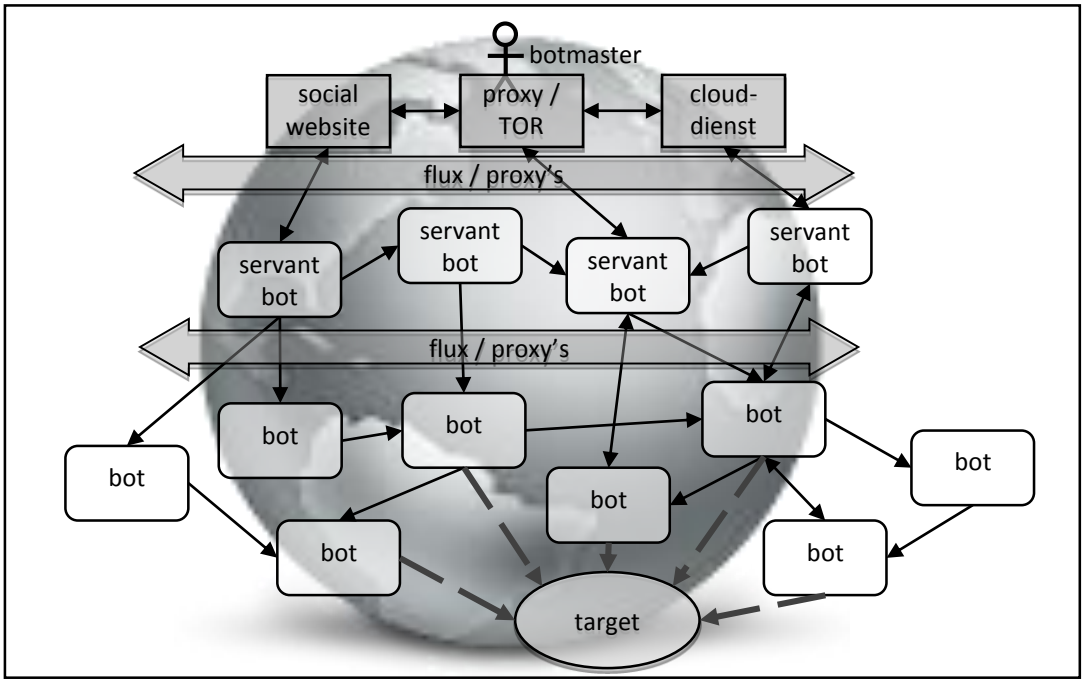
Sociale netwerken en de '*cloud'*, waarin computerdiensten onafhankelijk van elkaar worden aangeboden en waartussen diverse transparante communicatievormen mogelijk zijn zodat ze in verschillende dynamische

configuraties kunnen samenwerken, helpen botnets om een ideaal platform voor hun activiteiten te creëren (Yu, Zhou, Dou, & Makki, 2012).

Daarbij worden aanvullende technieken om de servers en bots te verbergen steeds meer gemeengoed. '*Fast-flux*' netwerken wijzigen enerzijds de domeinnaam van bots en servers continu ('*single flux*') en mogelijk ook de IP-adressen van de domeinnaamservers (DNS) die de domeinnamen van de bots en server bijhouden ('*double flux*'). In combinatie met '*domain flux*', waarbij de domeinnamen niet vastliggen maar in tijd veranderen, maken deze technieken het haast ondoenlijk om individuele bots en servers te achterhalen. Tevens wordt gebruik gemaakt van (reverse) proxy's om de servers af te schermen. (Zhu et al., 2008) (Fedynyshyn, Chuah, & Tan, 2011) (Tyagi & Aghila, 2011) (Zhang, Yu, Wu, & Watters, 2011).

Tot slot kunnen in een botnetstructuur de commando-, registratie- en gegevenskanalen worden gescheiden waarbij ieder kanaal gebruikt maakt van een best passende hybride structuur (Xiang et al., 2012).

Een mogelijke hybride botnet commandostructuur is weergegeven in Figuur 3.



Figuur 3. Schematische weergave van een botnet met hybride structuur, proxy's en flux

3.2.3. **Verspreiding van botnets**

Een vierde kenmerk op basis waarvan een indeling van botnets kan worden gemaakt is de wijze van infectie en verspreiding van botnets. Li, Jiang, & Zou (2009) beschrijven drie infectiemethoden:

- *web download*: websites kunnen zijn gemanipuleerd zodat een bezoeker zonder het te weten schadelijke software downloadt;
- *e-mail*: botnets worden gebruikt om spam en phishing e-mails te versturen met schadelijke software als bijlage;
- *scan, exploit and compromise*: bots scannen nabije computers op bekende zwakheden om zo een botagent naar binnen te brengen.

Deze infectiemethoden verschillen in principe niet van die van andere schadelijke software. Maar in tegenstelling tot een virus of worm zal de aankomende bot na de initiële infectie contact zoeken om de daadwerkelijke botagent te downloaden en te installeren, waarna de nieuwe bot zich kan registreren in het botnet en commando's kan uitvoeren.

3.2.4. **Indeling naar kenmerken**

In de vorige paragraaf zijn aan de hand van de definitie van een botnet een viertal eigenschappen besproken die kenmerkend zijn voor een botnet en daarmee mogelijk van belang voor de bestrijding ervan: het oogmerk of de intentie van de botmaster, de aanvalsvormen die het botnet kan benutten, de (commando)structuur van het botnet en tot slot de methoden om computers te infecteren.

Tyagi & Aghila (2011) geven onder meer op basis van Zhu et al. (2008) aan dat botnets over het algemeen worden ingedeeld naar commandostructuur. Voor botnetonderzoek en -bestrijding is dit ook de meest interessante eigenschap omdat het veel zegt over de sterktes, zwaktes en het gedrag van een botnet.

Preventie tegen infectie en verschillende aanvalsvormen zijn voor individuele personen en organisaties wel van belang voor bescherming tegen botnets, maar niet zozeer voor (de organisatie van) botnetbestrijding. Deze beide kenmerken zijn gezien het doel van dit onderzoek minder relevant.

Hoewel het oogmerk van de aanvaller niet uniek is voor botnets, is die eigenschap van belang gezien taken en bevoegdheden van mogelijk betrokken organisaties bij de botnetbestrijding.

3.3. **Bestrijdingmethoden voor botnets**

3.3.1. **Opsporing en detectie van botnets**

Botnets zijn vooral zichtbaar door drie activiteiten: verspreiding en infectie, verkeer van commandokanalen en aanvallen (Mendonça & Santos, 2012). Het opsporen en detecteren van botnets kan grofweg op twee verschillende manieren gebeuren: op actieve wijze door gebruik te maken van zogenaamde '*honeynets*', of passief door te zoeken naar bekende botnetpatronen of afwijkingen in software en in netwerkverkeer (J. Liu et al., 2009) (Tyagi & Aghila, 2011) (Raghava, Sahgal, & Chandna, 2012).

3.3.1.1. Actieve Methoden

Honeynets zijn omgevingen waarin kwetsbare computers of virtuele machines worden blootgesteld aan schadelijke software (de zgn. '*honeypots*'), zodat die vervolgens kan worden onderzocht door niet-geïnfecteerde systemen met daarvoor uitgeruste software (de zgn. '*honeywall*'). Een honeynet wordt vanwege het gerichte karakter hier primair als actief beschouwd, hoewel binnen een honeynet ook van passieve technieken gebruik kan worden gemaakt.

Rajab et al. (2006) beschrijven drie fasen waarin ze een botnet proberen op te sporen en te 'vangen':

- het verzamelen van schadelijke software door kwetsbare computers of virtuele machines;
- de schadelijke software testen om het gedrag en kenmerken te analyseren;
- het in kaart brengen van het botnet.

Ze waren met deze methode in staat 192 IRC botnets te vangen en kenmerken te analyseren, onder meer op geografische spreiding, gebruik van IRC-kanalen, netwerkgedrag, en gebruik van DNS. Met een honeynet kunnen real-time met relatief grote zekerheid botnets worden opgespoord (Raghava et al., 2012), maar het vraagt om een aanzienlijke investering in kennis en infrastructuur.

Actieve netwerk-gebaseerde technieken genereren datapakketten op het netwerk en gaan na of schadelijke software hierop reageert. Dit vereist dat de reactie van botnets enigszins bekend is; Raghava et al. (2012) vonden maar één actieve netwerktechniek die hiermee in staat was botnets te ontdekken.

3.3.1.2. Passieve methoden

Feily et al. (2009), Tyagi et al. (2011) en Raghava et al. (2012) beschrijven de in Tabel 4 weergegeven methoden voor het ontdekken van botnets.

Tabel 4. Passieve methoden voor de detectie van botnets

Signature-based detection	Wanneer karakteristieke kenmerken van een botnet exact bekend zijn, kan specifiek daarop worden gezocht. Dit is ook de wijze waarop veel antivirussoftware op een computer naar schadelijke software zoekt. Het nadeel is dat de eigenschappen van de botnets waarnaar wordt

	gezocht, bekend moeten zijn en dat onbekende botnets hiermee niet worden gevonden.
Anomaly-based detection	Deze wijze van detectie maakt gebruik van het feit dat botnets op een computer of in een netwerk afwijkend of onverwacht gedrag vertonen, bijvoorbeeld verhoogd gebruik van hulpbronnen, of ongebruikelijke netwerkverbindingen. Nadeel van deze methode is dat het normale gedrag van een systeem goed bekend moet zijn, of dat het detectiesysteem lerende eigenschappen moeten hebben om afwijkingen te kunnen constateren.
DNS-based detection	Het specifieke gebruik van DNS door botnets (zie paragraaf 3.2.2.3) maakt dat afwijkend DNS-verkeer voor de commandovoering van botnets kan worden herkend. Feitelijk betreft dit een specifieke vorm van *anomaly-based detection* specifiek op DNS gericht.
Network-based detection	Passieve netwerkgebaseerde technieken zijn bedoeld om in de inhoud van netwerkberichten typische botnetkenmerken of -patronen te ontdekken, zonder dat die exact bekend zijn. Zo zal de informatie die een bot met een IRC-bericht verstuurt, anders gestructureerd zijn dan een menselijk IRC-bericht.
Datamining-based detection	Buiten het DNS-verkeer zijn de commandovoeringskanalen van een botnet lastig te ontdekken, omdat ze weinig bandbreedte gebruiken en doorgaans normale protocollen. Dataminingtechnieken verzamelen een aanzienlijke hoeveelheid netwerkverkeer, clusteren en categoriseren het en zoeken naar correlaties of patronen die typisch zijn voor botnet, zoals tijdintervallen waarop ze bepaalde activiteiten vertonen.

3.3.1.3. Beperkingen bij de opsporing en detectie van botnets.

Zoals alle methoden kennen ook de hierboven beschreven detectievormen voor- en nadelen. Diverse bronnen beschrijven meer en mindere effectieve implementaties. Tabel 5 geeft een vergelijking van de methoden op basis van Feily et al. (2009) en Raghava et al. (2012). Om voor- en nadelen onderling te compenseren, moeten de methoden niet op zichzelf staand worden gezien; ze vullen elkaar aan. Zo worden passieve methoden ook binnen honeynets gebruikt en bestaan er op DNS gebaseerde detectietechnieken die gebruik maken van datamining (Zhang et al., 2011), en *darknets* waarin verdacht (*anomaly*) en/of geblokkeerd netwerkverkeer wordt afgevangen voor datamining (Zhu et al., 2008), et cetera.

Tabel 5. Vergelijking van botnetdetectiemethoden

Methode	Detectie van onbekende botnets	Commando-structuur-onafhankelijk	Detectie van vercijferde bots	Real-time	Bruikbaar op operationele netwerken	Minimale fout-positief[11]
Honeynet	X	X	X	X	-	X
Signature	-	-	-	-	X	-
Anomaly	X	-	X	-	X	-
DNS	X	-	X	X*	X	X
Network	X	X	X	-	X	-
Datamining	X	X	X	-	X	X*

* Feily et al. (2009) verwijzen naar studie-experimenten waarbij deze eigenschap wel bleek voor betreffende methode, terwijl Raghava et al. (2012) deze eigenschap niet toekennen aan deze methode.

Aviv & Haeberlen (2011) wijzen op een aantal generieke beperkingen van de beschreven methoden. Ten eerste is het onmogelijk een methode op het hele internet of zelfs een groot deel ervan toe te passen. Ten tweede is validatie van gepubliceerde methoden lastig om een aantal redenen: de broncode van de gebruikte detectiesoftware is vaak niet beschikbaar, het experiment kan niet exact worden gereproduceerd vanwege de veranderende omgeving (het Internet en de botnets zelf), en het is onmogelijk de resultaten van de experimenten met de werkelijkheid te vergelijken.

[11] Een 'fout-positief' is een zogenaamde type I fout: ten onrechte wordt aangenomen dat een botnet is gedetecteerd.

3.3.2. **In kaart brengen van botnets**

In het verlengde van opsporen en detecteren van botnets ligt het in kaart brengen van de (commando)structuur van een botnet, al dan niet ten dele binnen een kunstmatige omgeving zoals een honeynet. Maar naarmate de complexiteit van de (commando)structuur toeneemt, wordt het steeds moeilijker een botnet goed en volledig in kaart te brengen.

Dagon, Gu, Lee & Lee (2007) stellen voor een botnet te classificeren naar effectiviteit, efficiëntie en robuustheid, en definiëren hiervoor enkele metrieken voor de daadwerkelijke en effectieve grootte en de mate van connectiviteit binnen een botnet. Het is echter lastig deze grootheden te kwantificeren omdat ze sterk afhankelijk zijn van de beschikbare gegevens over een botnet. Vervolgens rijst de vraag hoe de gegevens op basis van de structuur en andere botnetkenmerken kunnen worden geëxtrapoleerd. Tot op heden zijn daar geen eenduidige en betrouwbare methoden voor (S. Liu, Gong, Yang, & Jakalan, 2011). Bovendien gebruiken botnets steeds vaker authenticatietechnieken, encryptie, en technieken die in staat zijn honeynets en gemanipuleerde *agents* te ontdekken (Lu et al., 2011).

Rajab, Zarfoss, Monrose & Terzis (2007) beschrijven twee methoden waarmee toch informatie kan worden verkregen:

- infiltereren: één of meer '*agents*', al dan niet in een honeynet, doen zich voor als een bot, en kunnen op die manier informatie verzamelen;
- botnetverkeer afvangen: botnets zijn afhankelijk van DNS, zodat door DNS-manipulatie botnetverkeer kan worden afgevangen of gerouteerd om te onderzoeken.

Twee andere manieren om een botnet grootschaliger in kaart te brengen zijn gebaseerd op overname van het botnet (Stone-Gross et al., 2009):

- door het commandokanaal af te vangen en te manipuleren, ook weer door DNS-manipulatie;
- door een commandoserver over te nemen (hacken).

Om deze methoden effectief toe te passen moet het gedrag van het botnet al enigszins bekend zijn. Het is met de huidige analysemethoden echter niet met zekerheid vast te stellen of op enig moment voldoende eigenschappen van botnets inzichtelijk zijn[12].

3.3.3. **Opsporen van de botmaster**

Wanneer het internetadres van een botmaster bekend is, kan worden vastgesteld waar de botmaster zich bevindt en kan met gegevens van de internetaanbieder mogelijk (de locatie van) het gebruikte netwerk, computer of individu worden geïdentificeerd. Voor eenvoudige botnets kan met het in kaart brengen mogelijk ook de botmaster worden achterhaald. Maar complexere botnets vragen om specifieke opsporingsmethoden omdat botmasters hun internetadres en zichzelf verborgen houden in de *cloud*, bijvoorbeeld achter sociale netwerken, proxy's, veranderende domeinnamen, servers en bots. Een botmaster kan bovendien van openbare (Wi-Fi) netwerken gebruik maken en daarmee meer internetadressen gebruiken. Om toch het internetadres te achterhalen zal een specifiek spoor vanaf een bot of server naar de botmaster moeten worden gevolgd.

Er zijn in afgelopen jaren diverse studies gedaan naar het traceren van internetverkeer. Het volgen van gemarkeerde datapakketten ('*watermarking*') is veelvuldig onderzocht, maar is te afhankelijk van de medewerking van internetaanbieders en de functionaliteit van netwerkapparatuur. Het biedt op netwerken van beperkte grootte, bijvoorbeeld van één internetaanbieder, wel mogelijkheden. Maar het is niet geschikt als oplossing voor het hele internet dat geen centrale autoriteit kent en bestaat uit veel aan elkaar gekoppelde netwerken over de hele wereld. Het is daarom zowel om technische, politieke als juridische redenen moeilijk het internetadres en vervolgens de identiteit van botmasters te traceren en te identificeren (Clark & Landau, 2010) (Yu et al., 2012).

Lin & Lee (2012) stellen een manier voor om de botmaster te traceren door te infiltreren in de '*stepping stones*' (opeenvolgende proxy's, clouddiensten, commandoservers, etc.) die een botmaster gebruikt om

[12] Om dezelfde redenen als in Paragraaf 3.3.1 beschreven op basis van Aviv et al. (2011).

een botnet aan te sturen. Met behulp van een '*traceback server*' waaraan geïnfiltreerde *stepping stones* rapporteren, wordt ingebrachte gemerkte informatie gevolgd om volgende *stepping stones* te achterhalen. Feitelijk wordt daarmee een gericht 'anti-botnet' gecreëerd door vanaf een bot de route terug naar een botmaster te volgen en de *stepping stones* te infecteren. Voorwaarde is ook hier dat de structuur en het functioneren van een botnet eerst goed in kaart wordt gebracht, bots informatie verzamelen en terugsturen en ook dat het berichtenverkeer van het botnet kan worden ontcijferd.

3.3.4. **Uitschakelen van een botnet**

Een botnet kan worden uitgeschakeld door individuele bots, de structuur of commandokanalen van het botnet of de botmaster aan te grijpen (Estrada & Nakao, 2010). Praktisch gezien is het echter onmogelijk alle bots in een botnet op te sporen, waardoor het aangrijpen van de botnetstructuur of opsporen van de botmaster het meest voor de hand ligt.

Voor botnets met een centrale commandostructuur is het effectief de commandoserver over te nemen, terwijl botnets met een decentrale commandostructuur te ontwrichten zijn door commandoberichten te manipuleren (Stone-Gross et al., 2009). Hierbij wordt voor de uitschakeling van een botnet feitelijk gebruik gemaakt van de in Paragraaf 3.3.2 beschreven methoden voor het in kaart brengen van botnets , maar nu om het botnet actief te manipuleren.

Als de botmaster kan worden opgespoord, op internet maar ook fysiek, kan deze mogelijk worden gestopt. De beschikbare en gewenste methoden om de botmaster te stoppen zijn afhankelijk van de beschikbare middelen en het oogmerk van de botmaster. Wanneer de botmaster zich binnen de jurisdictie bevindt van een meewerkend land, kunnen de commandoservers in beslag worden genomen, kan de botmaster worden gearresteerd en, afhankelijk van het beschikbare en toelaatbare bewijsmateriaal, worden berecht. Maar gaat het om cyberterrorisme of cyberoorlog, en werken autoriteiten niet mee, dan kan fysieke uitschakeling van de botmaster of van de gebruikte infrastructuur de meest effectieve manier zijn om een botnet te bestrijden.

Tot slot hoeven de bestrijdingsmethoden niet absoluut en definitief te zijn: een uitgeschakelde commandoserver kan een back-up in een ander land hebben, verstoring van een botnet kan negatieve effecten hebben op andere communicatie, en iemand anders kan de plaats van een gearresteerde botmaster innemen. Botnets zijn steeds meer ingericht om na ontregeling snel weer operationeel te zijn (Bleaken, 2010).

3.3.5. **Overzicht van bestrijdingsmethoden**

Op basis van het bovenstaande kunnen op hoofdlijn de in Tabel 6 weergegeven bestrijdingsmethoden worden geïdentificeerd.

Tabel 6. Botnetbestrijdingsmethoden

Aangrijp-ingspunt	Methode	Effectief tegen	Randvoorwaarden
Bot	Verwijderen bots uit het botnet (op een eigen netwerk).	In zichzelf niet effectief voor de bestrijding van een botnet; vooral preventief middel.	Signatuur van de botagent is bekend zodat deze wordt ontdekt door antivirussoftware.
Botnet-structuur	Overname of uitschakelen commandoserver(s)	(Eenvoudige) botnets met een centrale commandostructuur.	Werking van het botnet en (locatie van) commandoserver(s) zijn in voldoende mate bekend. Hostingproviders werken mee.
	Verstoring van het botnet met gemanipuleerde bots (zelfvernietigingsopdracht, vervuiling van gegevens).	(Complexere) botnets met een decentrale of hybride commandostructuur.	Werking van het botnet is goed bekend. Eventuele encryptiesleutels kunnen worden gekraakt. Men is in staat computers te infecteren met gemanipuleerde botagents, al dan niet gebruik makend van het oorspronkelijke botnet.

	Overname of verstoring van het botnet door manipulatie van de communicatie (zelfvernietigingsopdracht, vervuiling van gegevens, opdrachten van botmaster afvangen, blokkeren van domeinnamen en IP-adressen).	(Complexere) botnets met een decentrale of hybride commandostructuur.	Werking van het botnet is goed bekend. Eventuele encryptiesleutels kunnen worden gekraakt. Internet/DNS-aanbieders werken mee.
Botmaster(s)	Arresteren en vervolgen van de botmaster(s).	Botnets met als oogmerk: cybervandalisme (A), misdaad over internet (B), cybercriminaliteit (C) en hacktivisme (D) en cyberterrorisme (E)	De botmaster kan worden opgespoord met medewerking van autoriteiten en internetaanbieders in betrokken landen. Er kan voldoende bewijslast worden veiliggesteld.
	Botmaster(s) en/of opdrachtgevers en/of infrastructuur fysiek uitschakelen.	Botnets met cyberterrorisme (E) en cyberoorlog (F) als oogmerk.	Het internetadres en de fysieke locatie van de botmaster kunnen worden achterhaald met beperkte of zonder medewerking van autoriteiten en internetaanbieders in andere landen door middel van reguliere en bijzondere inlichtingenmethoden. De (militaire) capaciteit is beschikbaar, proportioneel en toereikend voor fysieke uitschakeling.

3.4. Competenties, bevoegdheden en organisaties voor de bestrijding van botnets

Een 'competentie' wordt hier beschouwd als het vermogen waarover een groep of organisatie beschikt om een bepaald, gemeenschappelijk doel te realiseren (M. Weggeman, 1997). In de context van dit onderzoek wordt dat vermogen gezien als de informatie, kennis, vaardigheden en middelen binnen een organisatie om de in Hoofdstuk 3.3 beschreven botnetbestrijdingsmethoden effectief toe te passen.

3.4.1. Competenties voor detectie en analyse

Uit de vorige onderzoeksvraag is gebleken dat detectie en analyse essentiële randvoorwaarden zijn voor botnetbestrijding. De hieronder weergegeven competenties voor detectie en analyse van botnets volgen uit de uitkomsten van vorige onderzoeksvraag.

Tabel 7. Competenties voor botnetbestrijding

C1. Het detecteren van bots en botnets op internet met een honeynet.
C2. Het detecteren van bots en botnets op een specifiek netwerk met passieve methoden.
C3. Het onderzoeken van specifieke malware (software van botagents) op gedrag en eigenschappen.
C4. Het onderzoeken van de eigenschappen en het gedrag van specifieke botnets: – met behulp van een honeynet; – door infiltratie met botagents; – door het afvangen van botnetdataverkeer; – door manipulatie van het commandokanaal; – door overname van een commandoserver.
C5. Het achterhalen van encryptiesleutels en ontcijferen van informatie.

De inventarisatie van deze competenties is op hetzelfde detailniveau als de uitkomsten van onderzoeksvraag [T.2]; verdere verdieping en uitsplitsing in subcompetenties vraagt om een analyseslag buiten het bereik van dit onderzoek.

3.4.2. **Competenties voor opsporing en uitschakeling**

Voor de opsporing van de botmaster en actieve bestrijding van botnets worden in aanvulling op de bovenstaande competenties, de volgende competenties onderkend.

Tabel 7 (vervolg). Competenties voor botnetbestrijding

C6. Het verwijderen van botagents van computers (op een eigen netwerk).
C7. Het overnemen van een commandoserver.
C8. Het verstoren van het botnet met gemanipuleerde bots.
C9. Het verstoren of blokkeren van het botnet door manipulatie van de communicatie.
C10. Het overnemen van het botnet door manipulatie van de communicatie.
C11. Het traceren van adressen / computers op internet.
C12. Het regulier opsporen van de botmaster: – door opsporingsinstanties in Nederland; – met medewerking van autoriteiten in het buitenland.
C13. Het in beslag nemen van een commandoserver / computermateriaal.
C14. Het veiligstellen van bewijsmateriaal (zowel fysiek als digitaal).
C15. Het arresteren en vervolgen van de botmaster(s).
C16. Op bijzondere wijze opsporen van de botmaster(s) in het buitenland.
C17. Het fysiek uitschakelen van botmaster(s) en/of infrastructuur.

Hoewel deze competenties en die uit de vorige paragraaf in eerste instantie in elkaars verlengde moeten worden gezien, is niet uitgesloten dat competenties tegenstrijdig kunnen zijn. Zo kan overnemen of verstoren van een botnet (C9), of het fysiek uitschakelen van botmaster en/of infrastructuur (C17) afbreuk doen aan het veiligstellen van bewijsmateriaal (C14).

3.4.3. **Aanvullende competenties**

Het is onwaarschijnlijk dat alle benodigde competenties en bevoegdheden binnen één organisatie bestaan. Bovendien hebben digitale aanvallen eigenschappen waardoor ze te complex zijn om op te reageren (Prins, 2012). Organisaties moeten daarom in staat zijn tot samenwerking en coördinatie, zowel nationaal als internationaal.

C18. Samenwerking en coördinatie voor botnetbestrijding.

Daarnaast is voor de ontwikkeling van de benodigde kennis ten behoeve van alle competenties (wetenschappelijk) onderzoek naar botnets nodig (naast het onderzoeken van specifieke botnets met competenties C3 en C4):

C19. (Wetenschappelijk) onderzoek (ten behoeve van alle andere competenties) op het gebied van botnetbestrijding.

3.5. Organisaties betrokken bij de bestrijding van botnets en hun bevoegdheden

De bij botnetbestrijding betrokken organisaties in Nederland en hun bevoegdheden worden in de paragrafen hieronder besproken. Er is daarbij een verdeling gemaakt in betrokken publieke en private organisaties. Tenzij anders is aangegeven, bestaat er geen hiërarchische relatie tussen de organisaties. Er is

in het literatuuronderzoek niet gekeken of de organisaties ook daadwerkelijk over de competenties beschikken en hoe die zijn georganiseerd; dat is wel in het empirisch deel onderzocht

3.5.1. **Publieke organisaties**

3.5.1.1. Nationale Coördinator Terrorismebestrijding en Veiligheid

De NCTV heeft tot taak dreigingen voor de vitale belangen van de samenleving te identificeren en de weerbaarheid en bescherming te versterken, onder meer op het gebied van cyber. Binnen de NCTV is het NCSC belast met de strategieontwikkeling, het realiseren van risicomanagement en het bevorderen van de publiek-private samenwerking op het gebied van cyber security (*Organisatieregeling Ministerie van Veiligheid en Justitie 2011*, 2011). De belangrijkste competentie voor deze organisatie is dus de samenwerking en coördinatie voor botnetbestrijding (C18).

3.5.1.2. Inlichtingen- en Veiligheidsdiensten

Nederland kent twee inlichtingen- en veiligheidsdiensten, een algemene (de AIVD) en een militaire (de MIVD), die tot taak hebben onderzoek te doen naar organisaties en personen die een mogelijk gevaar vormen voor de democratische rechtsorde, de veiligheid of andere gewichtige belangen. Beide diensten zijn niet bevoegd tot het opsporen van strafbare feiten, maar hebben wel een aantal andere bijzondere bevoegdheden. Daaronder valt het binnendringen van geautomatiseerde systemen, het aftappen van datacommunicatie en het ongedaan maken van eventuele versleuteling (*Wet op de inlichtingen- en veiligheidsdiensten 2002*, 2002). Er is echter geen expliciete bevoegdheid dat ook in het buitenland te doen (Ducheine & Voetelink, 2011).

Gezien hun taken zouden de inlichtingen- en veiligheidsdiensten voor onderzoek naar botnets met hacktivisme, cyberterrorisme, cyberoorlog en ernstige vormen van cybercriminaliteit als oogmerk over alle competenties voor detectie en analyse van botnets moeten beschikken (C1 t/m C5) en in het verlengde daarvan in ieder geval over de competenties om botmasters op te sporen: C6, C11, C12 en C16, waarbij competenties C5 en C16 unieke kerncompetenties van inlichtingendiensten zijn.

3.5.1.3. Openbaar Ministerie

Het OM is belast met de strafrechtelijke handhaving van de rechtsorde in Nederland (*Wet op de rechterlijke organisatie*, n.d.) en de officieren van justitie met de opsporing van strafbare feiten (*Wetboek van Strafvordering*, n.d.). Daaronder vallen in principe alle cyberaanvallen met botnets, met uitzondering van cyberoorlog en in voorkomend geval cyberterrorisme waar niet zozeer het strafrecht maar het volkenrecht op van toepassing is (Lodder & Boer, 2012). De feitelijke opsporing vindt onder gezag van het OM plaats door de politie. Wel heeft het OM een unieke taak in de vervolging van een botmaster (C15), in de nationale aansturing van een strafrechtelijk onderzoek naar een botnet, en bij internationale coördinatie (C18).

3.5.1.4. Politie

De politie is belast met handhaving van de rechtsorde binnen Nederland (*Politiewet 2012*, 2012). Daaronder valt de opsporing van strafbare feiten (*Wetboek van Strafvordering*, n.d.), ook in het cyberdomein (Stol, Leukfeldt, & Klap, 2012). De politie heeft haar cybercapaciteit geconcentreerd bij het Team High Tech Crime (THTC) van het Korps Landelijke Politiediensten (KLPD).

Competenties C11 t/m C15 voor het opsporen van de botmaster sluiten aan bij de kerntaak en bevoegdheid van de politie voor de opsporing van strafbare feiten. Eerder besproken is het belang van de competenties C1 t/m C5 voor detectie en analyse die ten grondslag liggen aan effectieve bestrijding. De vraag daarbij is wel of actief zoeken naar botnets (C1 en C2) primair door de politie zelf kan of moet gebeuren[13]. Dat neemt echter niet weg dat de politie wel in staat moet zijn uiteindelijk opsporingswerkzaamheden te verrichten en daarvoor toch over de kennis moet beschikken, ook al wordt een botnet eerst door anderen ontdekt.

[13] Het gebruik van een honeynet kan nog worden gezien als vorm van surveillance, maar de politie kan niet zonder toestemming botnets detecteren op netwerken van derden.

Nauw gerelateerd aan de analyse van een botnet (C4) zijn de competenties om ook het botnet uit te schakelen (C7 t/m C9), bijvoorbeeld voor herstel van de openbare orde en om te voorkomen dat na arrestatie van de botmaster een andere botmaster het botnet overneemt. Zowel voor opsporing als uitschakeling is het dus noodzakelijk dat men infiltreert in botnets en zich toegang verschaft tot computers die daar deel van uitmaken ('terughacken'). Maar voor deze competenties bestaat geen rechtsbasis (Koning, 2011).

Botnets en cyberdelicten kenmerken zich doordat ze grensoverschrijdend zijn. De politie is echter alleen in Nederland bevoegd, wat de politie noopt tot internationale samenwerking (C18), bijvoorbeeld via het European Cybercrime Centre (EC3) van Interpol in Den Haag.

3.5.1.5. Krijgsmacht

De krijgsmacht heeft de grondwettelijke taak het grondgebied en de belangen van de staat te beschermen (*Grondwet voor het Koninkrijk der Nederlanden*, n.d.). Hierin ligt impliciet de bestrijding van cyberdreigingen besloten wanneer die inbreuk maken op de integriteit van de samenleving. Daadwerkelijke inzet van de krijgsmacht ligt echter ingewikkeld vanwege de verschillende rechtsbases en rechtsregimes die er ten aanzien van militaire inzet bestaan en waarvan niet altijd duidelijk is in hoeverre die op het digitale domein toepasbaar zijn.

De krijgsmacht heeft een zelfstandige taak wanneer aanvallen met een botnet onderdeel uitmaken van een gewapend conflict, een militaire operatie in het buitenland, of een aanval op Nederland (cyberoorlog, en mogelijk cyberterrorisme). Maar het is niet duidelijk of een cyberaanval met een botnet op (vitale belangen van) een land juridisch gezien ook als een 'gewapende aanval' kan worden beschouwd. Want slechts dan is bestrijding van een botnet als zelfverdediging (inclusief fysieke uitschakeling van de botmaster) mogelijk zonder instemming van het land waarin een operatie plaatsheeft en zonder autorisatie van de VN-veiligheidsraad (Ducheine & Voetelink, 2011).

Binnen Nederland heeft de krijgsmacht in vredestijd een zelfstandige taak wanneer een botnetaanval zich direct tegen de krijgsmacht richt (ongeacht het oogmerk). De Nederlandse wetgeving voor bewaking van militaire objecten is echter gebaseerd op klassieke fysieke bewaking, en voorziet niet in een rechtsbasis voor actieve digitale verdediging (Ducheine & Voetelink, 2011). Wel heeft de Koninklijke Marechaussee als onderdeel van de krijgsmacht ten aanzien van de krijgsmacht dezelfde opsporingsbevoegdheden voor strafbare feiten als de civiele politie.

Naast genoemde zelfstandige taken, kan de krijgsmacht ook voor bijstand aan civiele autoriteiten worden ingezet wanneer omstandigheden daarom vragen. Dat gebeurt regelmatig op velerlei gebied[14] en is juridisch ook afgedekt (Ducheine & Voetelink, 2011). Daarnaast werkt de krijgsmacht vaak internationaal samen, meestal in NAVO-verband. Zo ook op dit terrein in het NATO Cooperative Cyber Defence (CCD) Centre of Excellence (COE) in Tallinn, Estland.

Met genoemde taken zou de krijgsmacht het volledige spectrum aan competenties moeten bezitten, waarbij C17 een unieke kerncompetentie van de krijgsmacht is, de competenties C12 en C15 specifiek samenhangen met de opsporingsbevoegdheid van de marechaussee, en de competenties voor detectie en analyse van botnets en opsporing van een botmaster ook al beschikbaar zouden moeten zijn bij de MIVD. Hoewel offensief gebruik van botnets buiten dit onderzoek valt, kan dat de krijgsmacht een extra competentiebasis geven.

[14] Martijn Delaere. (2012, August 31). Justitie en politie worden geholpen door Defensie. *Binnenlands Bestuur*. Retrieved January 4, 2013, from http://www.binnenlandsbestuur.nl/bestuur-en-organisatie/achtergrond/achtergrond/defensie-helpt-justitie-en-politie.8500587.lynkx

3.5.2. **Private organisaties**

3.5.2.1. IT-bedrijven

IT-bedrijven spelen een specifieke rol bij botnetbestrijding. Hieronder vallen zowel internetaanbieders[15] die faciliterend zijn voor IT-diensten, als computerbeveiligingsbedrijven die gespecialiseerd zijn in het opsporen en analyseren van malware. Ten aanzien van botnets zullen internetaanbieders zich primair op cybervandalisme en –criminaliteit richten. Computerbeveiligingsbedrijven, die ook de overheid en vitale bedrijven als klant hebben, zullen het hele spectrum moeten bestrijken.

Internetaanbieders moeten in ieder geval in staat zijn om botnets op hun netwerken te herkennen (C2). Beveiligingsbedrijven doen in brede zin onderzoek naar schadelijke software en cyberaanvallen (C1, C3, C4 en C18) en de bestrijding ervan (competenties C6 t/m C11). Voor deze competenties is ontcijfering van gegevens, infiltratie en/of overname van botnets vaak noodzakelijk, maar voor private organisaties geldt ontcijfering van gegevens, infiltratie en/of overname van botnets als computervredebreuk en dat is strafbaar (*Wetboek van Strafrecht*, n.d.). De competenties kunnen dus slechts beperkt worden toegepast, namelijk op eigen netwerken, en zelfs daar moeten internetaanbieders rekening houden met privacyregelgeving en heeft men niet zonder meer toegang tot opgeslagen gegevens van derden (Koning, 2011).

Gezien het niveau van integratie kan het beveiligen van netwerken niet los worden gezien van het op juiste wijze zekerstellen van bewijsmateriaal (Hunt & Slay, 2010). Dit maakt dat internetaanbieders en IT-beveiligingsbedrijven ook over de competenties daarvoor moeten beschikken (C14).

3.5.2.2. Vitale bedrijven

Onder vitale bedrijven worden ondernemingen verstaan die een cruciale taak voor de samenleving uitvoeren, zoals banken en elektriciteitsbedrijven, of die gezien hun aard meer dan gemiddeld gevoelig zijn voor cyberaanvallen, zoals digitale (bedrijfs)spionage. Zij zullen minimaal in staat moeten zijn om botnets te detecteren, al dan niet met een honeynet (C1, C2), en de dreiging zoveel mogelijk af te slaan (C6 en C9).

Bedrijven huren hiervoor steeds vaker gespecialiseerde IT-securitybedrijven in, inclusief particuliere recherchediensten (Prins, 2012). De vraag daarbij is in hoeverre zij hun competenties mogen aanwenden, omdat de mogelijkheden voor opsporing en uitschakeling zonder infiltratie en overname van een botnet beperkt zijn, doordat het computervredebreuk oplevert en/of een schending van de privacy door het verkrijgen van toegang tot gegevens van derden. Competenties C6, C8, C9 en C11 kunnen dus beperkt worden aangewend op eigen netwerken, al dan niet via een gespecialiseerd beveiligingsbedrijf. Voor volledige botnetbestrijding zal men moeten terugvallen op (de bevoegdheden van) publieke organisaties (Prins, 2012).

3.5.2.3. Niet-vitale bedrijven en particulieren

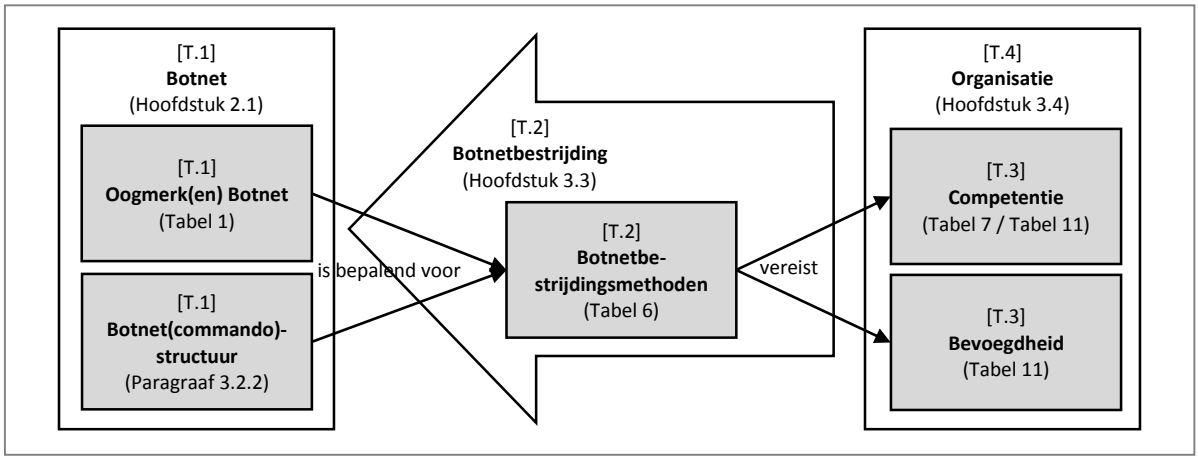
Vanwege de complexiteit van botnets en de benodigde competenties om ze te bestrijden, moet de rol van particulieren en niet-vitale bedrijven als beperkt worden beschouwd. Hoogstens beschikken ze met hulp van gespecialiseerde bedrijven over software om botnets op eigen systemen te ontdekken (C2) en infecties met malware te verwijderen (C6).

[15] Onder 'internetaanbieder' wordt hier niet alleen verstaan een bedrijf dat anderen toegang tot het internet verschaft, maar alle internetdiensten, inclusief DNS-aanbieders, hostingproviders, clouddiensten, etc.

3.6. Referentiemodel voor botnetbestrijding

3.6.1. Conceptueel model en Referentiemodel

De uitkomsten van het literatuuronderzoek zijn te vatten in een conceptueel model en in een referentiemodel. Figuur 4 laat het conceptuele model zien dat weergeeft hoe de relevante aspecten van het onderzoek samenhangen: het oogmerk van het botnet en de botnetstructuur zijn de twee eigenschappen van botnets die bepalend zijn voor de bestrijdingsmethoden van het botnet, die vervolgens bepaalde competenties en bevoegdheden vereisen van de betrokken organisaties. Dit model is grotendeels inherent aan de opzet van de onderzoeksvragen.



Figuur 4. Conceptueel model voor de organisatie van botnetbestrijding in Nederland.

Het referentiemodel is feitelijk een meerdimensionaal model dat voor de Nederlandse situatie de relaties weergeeft tussen de verschillende aspecten (dimensies) van botnetbestrijding die in dit rapport zijn uitgewerkt op basis van de onderzochte literatuur. Het referentiemodel is dus een concretisering van het conceptuele model. Het is weergegeven met behulp van twee tabellen in Bijlage D: Tabel 10 legt de relatie tussen de dimensies bestrijdingsmethode, commandostructuur, oogmerk en competenties; Tabel 11 legt de relatie tussen de dimensies organisatie, oogmerk, competenties en bevoegdheden.

3.6.2. Validatie van het referentiemodel

In Figuur 4 is aangegeven welk element in het conceptuele model, en daarmee welke dimensie van het referentiemodel, aan welke theoretische onderzoeksvraag is gerelateerd. Zoals te zien is, zijn alle theoretische onderzoeksaspecten in de modellen afgedekt. Beide theoretische modellen laten daarmee niet zien in hoeverre de benodigde competenties bij Nederlandse organisaties aanwezig zijn en gezamenlijk kunnen worden ingezet, maar bieden wel de basis voor gericht empirisch onderzoek.

Het empirisch deel van het onderzoek heeft tot doel te toetsen of het gepresenteerde referentiemodel in Bijlage D overeenkomt met de wijze waarop in Nederland de botnetbestrijding is georganiseerd. Daarbij wordt na operationalisatie van de variabelen van het model gekeken hoe verschillen tussen het model en de werkelijkheid kunnen worden verklaard: zijn afwijkingen tussen het model en de werkelijkheid omissies in het model of een hiaat in de organisatie van de bestrijding van botnets?

4. Empirische onderzoeksresultaten van botnetbestrijding

4.1. Introductie

Het empirisch deel van het onderzoek heeft tot doel te toetsen of het referentiemodel voor botnetbestrijding compleet en correct is. Daartoe wordt het referentiemodel vergeleken met de Nederlandse werkelijkheid. Het onderzoek is uitgevoerd met een semigestructureerd interview. Paragraaf 4.2 beschrijft kort de onderzochte organisaties zoals zij zich in het interview hebben gepresenteerd, waarna in Paragraaf 4.3 wordt ingegaan op de botnetbestrijding door deze organisaties.

Een overzicht van geïnterviewde personen is te vinden in Bijlage B. De door de geïnterviewden goedgekeurde interviewverslagen staan in Bijlage F.

4.2. Interviews

4.2.1. Nationaal Coördinator Terrorismebestrijding en Veiligheid en het Nationaal Cyber Security Centrum

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft de taak om dreigingen te identificeren en te verminderen, om de weerbaarheid te versterken en om crisisbeheersing uit te voeren op de gebieden van terrorismebestrijding, nationale veiligheid en cyber security. De NCTV voert deze taak vanuit een centrale coördinerende positie uit met diverse andere organisaties. Het NCSC valt onder de Directie Cyber Security van de NCTV. Het NCSC richt zich op het leveren van inzicht en het bieden van handelingsperspectief aan overheidsinstanties en vitale bedrijven op het gebied van cyberdreigingen. Het NCSC kent drie afdelingen: Expertise & Advies, Monitoring & Respons en Ontwikkeling & Programma's (Sande, Woutersen, & Leeuwen, 2013).

De NCTV en het NCSC ontlenen hun bestaan aan de organisatieregeling van het Ministerie van Justitie; zij hebben geen expliciete wettelijke taken of bevoegdheden. Een deel van de taken van de NCSC is die van de *National Computer Emergency Response Team* (National CERT)[16].

4.2.2. Openbaar Ministerie

Bij het Openbaar Ministerie is specifiek het Landelijk Parket onderzocht. Dat parket bestrijdt (inter)nationaal georganiseerde misdaad en geeft leiding aan de opsporingsonderzoeken van de Nationale Recherche. Men richt zich in het bijzonder op de internationale handel in en smokkel van mensen, cocaïne, heroïne, vuurwapens en explosieven, de productie en export van synthetische drugs, witwassen van misdaadgeld, terrorisme en *high tech crime*. Het landelijk parket heeft één officier van justitie die zich specifiek met cybercrime bezig houdt en een klein juridisch kennis- en expertisecentrum op het gebied van cyber. (Zwieten, 2013)

4.2.3. Politie

De politie beschikt over het Team High Tech Crime dat deel uitmaakt van de Nationale Recherche. Het THTC voert onder gezag van het OM opsporingsonderzoek uit. Merk op dat niet alle botnets als '*hightech'* worden aangemerkt. Het THTC groeit naar ongeveer 120 personen in 2014, zodat er tussen 15 en 20 grote zaken per jaar kunnen worden gedaan. Het is niet bekend of dit voldoende is om alle botnets effectief te kunnen bestrijden, ook omdat ook andere hightech criminaliteit hiermee moet worden bestreden en het onbekend

[16] Computer Emergency Response Teams (CERTs) of Computer Security Incident Response Teams (CSIRTs) zijn organisaties die op basis van de *best practices* van de RFC2350 dan wel door het Software Engineering Institute (SEI) van de Carnegie Mellon University zijn goedgekeurd om veiligheidsincidenten van computersystemen en –netwerken te bestrijden. Veel CERTs werken samen in het Forum of Incident Response and Security Teams (FIRST) en er bestaat ook een samenwerkingsverband van Europese Government Certs (EGC). Zie onder meer: http://www.cert.org/csirts/csirt_faq.html.

is hoeveel botnets er precies zijn. Het THTC zal dan bestaan uit drie operationele teams (bestaand uit ieder twee secties) die ieder over alle expertise beschikken om zelfstandig een zaak te kunnen onderzoeken. Een vierde team zorgt voor de interne ondersteuning, voorbereiding en beleid. Bij het THTC is tevens de Electronic Crime Task Force (ECTF) ingebed, een multidisciplinair team dat met de banken samenwerkt. (Maas, Bernaards, Wagenaar, & Graaf, 2013)

4.2.4. **Defensie**

Bij het Ministerie van Defensie is het Defensie Computer Emergency Response Team (DefCERT) onderzocht. DefCERT bestaat uit 15 personen georganiseerd in twee afdelingen. De afdeling Advies & Ondersteuning richt zich op advies voor CIS / ICT-beheers- en projectorganisaties binnen het Ministerie van Defensie en de krijgsmacht. De afdeling Incident Response houdt zich bezig met de analyse van beveiligingsincidenten van systemen in gebruik bij het Ministerie van Defensie en de krijgsmacht. (Eijk, 2013)

Van belang hierbij is dat DefCERT behoort tot de afdeling Informatievoorziening & Technologie (IVENT) van de Defensie Materieel Organisatie (DMO). Dat is een ondersteunende dienst die niet onder de Commandant der Strijdkrachten (CDS) valt en daarom niet tot de krijgsmacht behoort[17]. De rol van DefCERT moet daarom worden geïnterpreteerd als die van een vitaal bedrijf.

4.2.5. **Fox-IT**

Fox-IT is een privaat computerbeveiligingsbedrijf met ongeveer 200 werknemers. Het bedrijf maakt technische oplossingen en levert diensten op het gebied van cyberbeveiliging van overheidsinstanties en vitale bedrijven. De activiteiten van de organisatie vinden op drie niveaus plaats: Strategie, Operations en Infrastructuur. De infrastructuuractiviteiten richten zich op hardware- en netwerkoplossingen, zoals cryptografie en datadiodes. Operations houdt zich bezig met *incident response*, forensisch onderzoek etc. De strategieactiviteiten richten zich vooral op consultancy en computerbeveiligingsbeleid. (Prins, 2013)

4.3. **Uitkomsten van de interviews**

4.3.1. **Organisaties betrokken bij botnetbestrijding**

De gehouden interviews bevestigen dat de organisaties uit het referentiemodel de belangrijkste partijen zijn die in Nederland botnets bestrijden. Ook de betrokkenheid en rollen van organisaties die niet in het empirisch onderzoek zijn meegenomen, zoals de krijgsmacht en inlichtingendiensten, werden bevestigd door de geïnterviewden.

Daarnaast kunnen uit het empirisch onderzoek nog andere organisaties worden geïdentificeerd die een rol spelen bij botnetbestrijding. Ten eerste is er een aantal partijen dat weliswaar geen rol op de voorgrond bij botnetbestrijding speelt, maar er in bepaalde gevallen wel een specifieke rol speelt. Dit zijn:

- Nederlands Forensisch Instituut (NFI), een publieke organisatie die ondersteuning en onafhankelijke expertise levert door analyse en duiding van bewijsmateriaal;
- Stichting Internet Domeinnaamregistratie Nederland (SIDN), die zorgt voor de registrate van .nl domeinnamen, maar ook een open en veilig internet stimuleert;
- Ministerie van Economische Zaken, dat private initiatieven op het gebied van cybersecurity stimuleert;
- De Autoriteit Consument en Markt (ACM), die belast is met toezicht op telecommunicatie en bijvoorbeeld boetes kan opleggen voor het verzenden van spam.

[17] Ook uit andere zaken blijkt het (juridisch) verschil in status tussen de krijgsmacht en andere onderdelen van Defensie. Zo oordeelde de Hoge Raad dat het begrip 'strijdkrachten' (en 'krijgsmacht' als synoniem daarvan) beperkt dient te worden uitgelegd en dat daaronder niet "het Ministerie van Defensie als zodanig noch diens ondersteunende diensten" kunnen worden begrepen (*Opsporingsbevoegdheid opsporingsambtenaren Koninklijke marechaussee*, 2010).

Ten tweede refereren diverse geïnterviewden aan samenwerkingsverbanden op het gebied van computerveiligheid en botnetbestrijding. Deze verbanden variëren van formele werkgroepen tot fora voor officieuze informatie-uitwisseling. Het ligt buiten het doel van dit onderzoek om die volledig in kaart te brengen, maar als geheel vervullen ze zowel nationaal als internationaal een wezenlijke rol in de botnetbestrijding.

4.3.2. **Botnettaxonomie**

In het literatuuronderzoek worden botnets enerzijds geclassificeerd naar het oogmerk van het botnet, en anderzijds naar de commandostructuur. In het empirisch onderzoek is gekeken of de onderzochte organisaties eenzelfde (soort) indeling hanteren bij de bestrijding van botnets. Tabel 8 bevat hiervan de uitkomsten.

Tabel 8. Classificatie van botnets door onderzochte organisaties

Onderzochte organisatie	Taxonomie		
	Indeling naar oogmerk	Indeling naar commandostructuur	Andere indeling
NCTV / NCSC	Niet primair van belang bij bestrijding van een specifiek botnet. Beleidsmatig wel van belang voor kennisopbouw en om de juiste focus te leggen.	Niet primair van belang bij bestrijding van een specifiek botnet. Beleidsmatig wel van belang voor kennisopbouw en om de juiste focus te leggen.	Bij de bestrijding van botnets worden per geval de belangrijke aspecten bekeken.
Openbaar Ministerie	Indirect van belang ter beoordeling van toepasselijkheid van het strafrecht en het effect dat met het strafbare feit wordt bereikt.	Indirect van belang bij de haalbaarheid van de strafrechtelijke vervolging.	Het strafbare feit is leidend.
Politie	Niet primair van belang bij bestrijding van een specifiek botnet. Beleidsmatig wel van belang om de juiste focus te leggen.	Niet van praktisch belang; de gebruikte commando-structuren bij de zwaardere criminaliteit blijken in de praktijk relatief eenvoudig.	De aanvalsvorm (het strafbare feit) is leidend.
Defensie (als vitale organisatie)	DefCERT hanteert geen onderscheid naar oogmerk.	DefCERT hanteert geen onderscheid naar commando-structuur.	DefCERT maakt vooral onderscheid op basis van de uitgebuite zwakheden.
Fox-IT (computerbeveiligings-bedrijf)	Indirect van belang bij de bepaling welke overheidsinstantie bevoegd is.	Niet van praktisch belang; de gebruikte commando-structuren blijken in de praktijk relatief eenvoudig.	Geen specifieke indeling; bij de bestrijding van botnets worden per geval de belangrijke aspecten bekeken.

Alle organisaties geven aan dat bij de bestrijding van een specifiek botnet niet wordt gewerkt op basis van een vooraf bestaande indeling of taxonomie van botnets, omdat per geval en context bepaalde aspecten meer of minder belangrijk kunnen zijn. Als er al een indeling van botnets wordt gemaakt, dan is dat doorgaans:

- naar locatie: voor NCSC, OM en politie is het van belang of de botmaster of de gebruikte infrastructuur zich in Nederland bevindt;
- naar aanvalsvorm of strafbaar feit: voor OM en politie is dat het uitgangspunt voor handelen;
- naar uitgebuite zwakheden: voor DefCERT (en andere vitale organisaties) van belang omdat zij zich vooral richten op bescherming van de eigen systemen.

Een indeling naar oogmerk blijkt echter wel beleidsmatig van belang. De onderzochte organisaties gebruiken het impliciet voor kennisopbouw en om de juiste focus te leggen; zij gebruiken de indeling ook om houvast te bieden, om de verantwoordelijkheidsgebieden af te bakenen en om prioriteiten te stellen.

Een indeling naar commandostructuur wordt nagenoeg niet gehanteerd door de onderzochte organisaties, voornamelijk omdat het merendeel van de botnets nog van relatief eenvoudige centrale commandostructuren gebruik maakt.

4.3.3. **Botnetbestrijdingsmethoden**

In Paragraaf 3.3 zijn op basis van het literatuuronderzoek de botnetbestrijdingsmethoden van het referentiemodel beschreven. Hieronder worden de empirische bevindingen uit de interviews over deze bestrijdingsmethoden weergegeven.

4.3.3.1. Verwijderen bots uit het botnet

Uit de interviews blijkt dat geen van de onderzochte organisaties zich actief bezig houdt met het verwijderen van bots uit botnets. Wel hebben NCSC en DefCERT een signalerende en adviserende rol richting computer- en netwerkbeheerders van overheidsinstanties, internetaanbieders en vitale bedrijven. Zij kunnen bots uit hun netwerken verwijderen en kwetsbaarheden van computersystemen wegnemen, afhankelijk van het dreigingsbeeld of aan de hand van trendanalyse. (Sande et al., 2013)(Eijk, 2013)

In sommige gevallen gebruikt de politie, als onderdeel van hun hulpverlenende taak, een overgenomen botnet om besmette computergebruikers te informeren dat men is besmet. (Maas et al., 2013)(Zwieten, 2013)

4.3.3.2. Overname of uitschakelen commandoserver(s)

Het overnemen of uitschakelen van de commandoserver kan door middel van 'terughacken', beslagname of via een zogenaamde '*notice-and-take-down*' (NTD) procedure. Uitsluitend het OM acht zich bevoegd tot terughacken in gevallen waar dat proportioneel is (Zwieten, 2013). Civiele of strafvorderlijke beslagname en de NTD-procedure zijn ook middelen om een commandoserver uit de lucht te halen, maar beperken zich tot botnets met een commandoserver in Nederland (Sande et al., 2013).

4.3.3.3. Verstoring van het botnet met gemanipuleerde bots

Deze bestrijdingsmethode is met name effectief voor botnets met een decentrale commandostructuur. Omdat veel botnets nog steeds een centrale commandostructuur hebben, wegen de benodigde kennis en middelen van deze bestrijdingsvorm niet op tegen de verwachte beperkte resultaten. (Maas et al., 2013) (Prins, 2013)

4.3.3.4. Overname of verstoring van het botnet door manipulatie van de communicatie

Overname van een botnet door manipulatie van de communicatie, feitelijk een *man-in-the-middle attack* gericht tegen een botnet, wordt door geen van de onderzochte organisaties gedaan. Daarentegen komt verstoring van de communicatie van het botnet wel voor. In alle gevallen gaat het dan om *sinkholing*: de bot wordt onbereikbaar gemaakt op het netwerk (door het blokkeren van IP-poorten of manipulatie van DNS) waardoor de commando's van de botmaster de bots niet meer bereiken. Dit kan op private netwerken, of medewerking van internetaanbieders is vereist (Maas et al., 2013) (Sande et al., 2013) (Eijk, 2013)

4.3.3.5. Arresteren en vervolgen van de botmaster(s).

Het arresteren en vervolgen van de botmaster is de hoofdtaak voor het OM en de politie. De 'botmaster' moet hier breed worden gezien: dit kan degene zijn die technisch de controle over het botnet heeft, maar ook de persoon of organisatie die het botnet huurt (Maas et al., 2013).

Het aangrijpen van de botmaster is voor een private partij doorgaans geen effectieve bestrijdingsmethode, omdat de eerste prioriteit ligt bij het wegnemen van de aanval of de dreiging en bij het opheffen van de storingen. (Prins, 2013)

4.3.3.6. Botmaster(s) en/of opdrachtgevers en/of infrastructuur fysiek uitschakelen.

Geen van de onderzocht organisaties bedient zich van deze bestrijdingsmethode. De krijgsmacht en inlichtingendiensten zijn echter niet onderzocht.

4.3.4. **Bevoegdheden en competenties**

Bij de onderzochte organisaties kwamen de volgende afwijkingen van de in Paragraaf 3.4 beschreven bevoegdheden en competenties van het referentiemodel naar voren.

4.3.4.1. Competenties van NCSC en DefCERT

Het NCSC heeft naast de coördinerende rol ook een actieve signaleringsrol als nationale CERT voor de ontdekking van botnets die de IT-infrastructuur van de overheid en van vitale bedrijven bedreigen. De daarbij behorende competenties staan niet in het referentiemodel (Sande et al., 2013):

- Het NCSC kan bots en botnets op internet detecteren met een honeynet (C1), maar men maakt hoofdzakelijk gebruik van de gegevens van bestaande (non-profit / open source) honeynets en filtert de gegevens daarvan op IP-adressen in Nederland;
- Het NCSC is in staat bots en botnets te detecteren op een specifiek netwerk met passieve methoden (C2), en is dit momenteel aan het uitbreiden met een Nationaal Detectienetwerk voor de overheid en vitale infrastructuur;
- Het NCSC kan specifieke malware (software van botagents) onderzoeken (C3) op gedrag en eigenschappen, en traceert ook verdacht verkeer van adressen / computers op internet (C11).

DefCERT beschikt over dezelfde competenties, op basis waarvan kan worden gesteld dat (CERTs van) vitale bedrijven ook daarover beschikken (Eijk, 2013). Een verschil tussen de beide CERTs is dat DefCERT zelf actiever de botnets analyseert (C4), waar het NCSC meer gebruik maakt van gegevens die zij van derden krijgt of dit overlaat aan de partijen die zij over het bestaan van een botnet informeren (politie, internetaanbieder of vitaal bedrijf). In beide gevallen blijkt dat honeynetdetectie en malware-onderzoek voor alle bestrijdingsvormen, dus ook voor het verwijderen van bots uit een botnet, relevant is.

4.3.4.2. Ontcijferen

Het THTC en private computerbeveiligingsbedrijven, zoals Fox-IT, zijn in staat om te ontcijferen. In het algemeen is de vercijfering òf eenvoudig te kraken (bijvoorbeeld omdat sleutels *hardcoded* zijn en met reverse engineering snel achterhaald kunnen worden), òf te moeilijk om te kraken. (“High Tech Crime: Criminaliteitsbeeldanalyse 2012”, 2012)(Maas et al., 2013)(Prins, 2013)

4.3.4.3. Overnemen van een commandoserver

Terughacken is zich zonder toestemming toegang verschaffen tot een computersysteem om het botnet over te nemen (C7). Hoewel private computerbeveiligingsbedrijven en sommige overheidsinstanties als de politie hiertoe in staat zijn, is dit wettelijk niet toegestaan. Het OM oordeelt echter dat in sommige gevallen dit ‘terughackverbod’ niet opweegt tegen de schade of rechtsinbreuk die een botnet veroorzaakt. In dat geval kan het OM het overnemen van de commandoserver als een proportioneel middel beschouwen, waarbij dat middel uitsluitend door de overheid mag worden ingezet vanwege de proportionaliteitsafweging en het afleggen van verantwoording daarover als publieke organisatie. Momenteel wordt gewerkt aan wetswijzigingen die dit explicieter regelen. (Maas et al., 2013)(Zwieten, 2013)(Minister van Justitie, 2012)

Private partijen daarentegen willen ook zelf actiever optreden tegen botnets om hun eigen belangen veilig te stellen. De winst die nog zou kunnen worden bereikt uit meer investeringen in computerbeveiliging, weegt niet meer op tegen zelf actief aan botnetbestrijding te doen. Hoewel computerbeveiligingsbedrijven in staat zijn tot ‘terughacken’, belet de huidige wetgeving private organisaties om dat te doen. Dat geldt overigens niet alleen voor het overnemen en uitschakelen van botnets (C7), maar strikt genomen ook voor lichtere vormen van gegevensvergaring waarbij toch enige mate van inmenging in een botnet is vereist (C4). (Prins, 2013)(Koops, 2013)

4.3.4.4. Opsporen van de botmaster

Het THTC geeft aan dat het opsporen van de botmaster (C12) doorgaans met klassieke middelen plaatsvindt. Opsporing in het buitenland vindt plaats middels rechtshulpverzoeken (Maas et al., 2013). Fox-IT bevestigt het belang van het gebruik van traditionele opsporingsmethoden, omdat het zelfs voor een computerbeveiligingsbedrijf vaak mogelijk is om vanuit een goede inlichtingenpositie op basis van open bronnen een botmaster te achterhalen (Prins, 2013).

4.3.4.5. Beslaglegging en Notice-and-Take-Down

De in paragraaf 4.3.3.2 genoemde NTD-procedure kan resulteren in het offline halen van een server, waarbij de internetaanbieder, waaronder *hosting providers*, de toegang tot en de beschikking over de gegevens ontzegt aan de gebruiker (de botmaster). Hoewel dat geen beslaglegging in juridische zin is, kan deze competentie worden geschaard onder het beslagleggen (C13); deze competentie is in het referentiemodel echter niet toegeschreven aan internetaanbieders. (Sande et al., 2013)

Hoewel internetaanbieders in beginsel de gegevens van hun klanten niet actief inspecteren, biedt de NTD-procedure andere partijen (zoals het NCSC namens de overheid, private organisaties en particulieren) de mogelijkheid een klacht ('*notice*') in te dienen. Op basis hiervan kan de internetaanbieder onderzoeken of er daadwerkelijk sprake is van illegale activiteiten en deze stoppen door een server offline te halen ('*take-down*'), of beslag te leggen op de server of de gegevensbestanden (C13). (Sande et al., 2013)("Factsheet Notice-and-Take-Down", n.d.).

4.3.4.6. Niet voorkomende competenties

Een aantal competenties is bij geen van de onderzochte organisaties geconstateerd. Geen van de onderzochte organisaties maakt gebruik van verstoring van botnets met gemanipuleerde bots (C8) of overname van een botnet door manipulatie van de communicatie (C10). De competenties om botmasters op bijzondere wijze in het buitenland op te sporen (C16) en het fysiek uitschakelen van botmaster(s) en/of infrastructuur (C17) worden niet verder beschouwd, omdat de krijgsmacht en inlichtingendiensten niet zijn onderzocht.

4.3.5. **Organisatie van botnetbestrijding**

Uit de interviews blijkt het grote aantal organisaties dat bij botnetbestrijding is betrokken. Als we naast de overheidsorganisaties alle computerbeveiligingsbedrijven, internetaanbieders inclusief hostingsproviders, vitale bedrijven en internationale publieke en private organisaties beschouwen, gaat het om tientallen organisaties.

Binnen deze verzameling van organisaties bestaat een beperkt aantal structurele samenwerkingsverbanden, bijvoorbeeld de wettelijke relatie tussen het OM en de politie, internationale rechtshulpverzoeken, en de uitwijkmogelijkheden die DefCERT voor het NCSC biedt. Feitelijk zijn dit wettelijke samenwerkingsvormen die niet anders zijn dan voor andere domeinen dan cyber. Zo ook als er sprake is van een gedwongen samenwerking, bijvoorbeeld als er een gerechtelijk bevel is om een commandoserver offline te halen of te blokkeren.

Overige samenwerkingsvormen zijn meer projectmatig of ad hoc. De onderlinge afhankelijkheid tussen de organisaties is desalniettemin groot. Dat blijkt bijvoorbeeld omdat aan de ene kant de bevoegdheid tot aanwending van een aantal cruciale competenties uitsluitend bij de overheid ligt, met name verregaand onderzoek aan een botnet en het overnemen van een server ("OM Jaarbericht 2012", 2013)(Zwieten, 2013), terwijl aan de andere kant de overheid botnetbestrijding niet kan uitvoeren zonder de kennis en directe medewerking van internetaanbieders, computerbeveiligingsbedrijven en vitale bedrijven, die de technische kennis en zeggenschap over hun eigen netwerken hebben.

Ook de uitwisseling van actuele en accurate informatie is cruciaal bij botnetbestrijding (Sande et al., 2013)("Kennisdocument Taurus", 2011), evenals afstemming van belangen: heeft uitschakeling van het botnet prioriteit om de schade te beperken of ligt de prioriteit bij het vervolgen van de botmaster? (Zwieten, 2013) (Prins, 2013).

Alle geïnterviewden zijn van mening dat, gezien het grote aantal betrokken partijen, de botnetbestrijding niet anders dan in de huidige multilaterale samenwerkingsverbanden moet worden vormgegeven, waarbinnen iedere organisatie zijn rol moet kunnen invullen. Deze multilaterale samenwerking is voor een belangrijk deel gebaseerd op vertrouwen en erkenning van wederzijdse belangen, wat onder meer blijkt uit het feit dat de samenwerking meestal op een niet-verplichtende wijze wordt ingericht: (inter)nationale werkgroepen en liaisonfunctionarissen. Het NCSC speelt in dit netwerk van betrokken partijen een belangrijke verbindende rol, zowel tussen nationale en internationale organisaties, maar ook tussen publieke en private partijen.

Bij alle onderzochte organisaties vindt een verschuiving plaats van een hoofdzakelijk reactieve respons op botnets die door omstandigheden worden ontdekt, naar een meer proactieve aanpak om met betrokken partijen continu botnets in kaart te brengen, botnetgegevens uit te wisselen en botnets te bestrijden (Maas et al., 2013) (“OM Jaarbericht 2012”, 2013).

5. Conclusies en aanbevelingen

5.1. Conclusies uit het literatuuronderzoek

Er is aan de hand van een viertal theoretische onderzoeksvragen onderzocht welke organisaties, met welke competenties en bevoegdheden, nodig zijn voor een effectieve bestrijding van botnets op basis van karakteristieke eigenschappen van het fenomeen.

[T.1] *Welke soorten botnets kunnen op basis van hun eigenschappen worden onderscheiden*?

[T.2] *Welke methoden kunnen worden onderscheiden voor de bestrijding van botnets?*

Uit onderzoeksvraag [T.1] blijkt een botnet diverse kenmerkende aspecten te hebben. Van alle aspecten is een indeling naar enerzijds commandostructuur en anderzijds het oogmerk van het botnet het meest relevant om te bepalen welke (combinatie van) bestrijdingsmethoden voortkomend uit onderzoeksvraag [T.2] mogelijk effectief zijn.

De bestrijdingsmethoden zijn in te delen in methoden die individuele bots bestrijden, methoden die de botnetstructuur aangrijpen en methoden die zich richten op de botmaster. Het is hierbij van belang te beseffen dat er geen allesomvattende methode voor detectie, analyse en bestrijding van botnets bestaat. Afhankelijk van de opzet en complexiteit van het botnet is altijd een combinatie van methoden nodig om een botnet op te sporen, in kaart te brengen en te bestrijden. Honeynets in combinatie met DNS- en datamining-gebaseerde methoden lijken de meest effectieve manier om met een lage fout-positief botnets te detecteren. Voor het goed in kaart brengen van een botnet en de opsporing en uitschakeling van de botmaster, is manipulatie in meer of minder mate noodzakelijk, zoals afvangen van gegevensverkeer, infiltratie of zelfs overname van een botnet.

[T.3] *Welke competenties en bevoegdheden zijn nodig voor de toepassing van de geïdentificeerde bestrijdingsmethoden [T.2]?*

[T.4] *Welke soorten organisaties zouden betrokken moeten zijn bij een effectieve bestrijding van botnets, gegeven de geïdentificeerde benodigde competenties en bevoegdheden [T.3]?*

Aan de hand van onderzoeksvragen [T.3] en [T.4] zijn in Hoofdstuk 3.4 de competenties en bevoegdheden geïdentificeerd waarover publieke en private organisaties moeten beschikken om botnets te bestrijden met de in Hoofdstuk 3.3 onderkende methoden. De samenhang tussen de competenties en bevoegdheden van de organisaties die in Nederland betrokken zijn bij botnetbestrijding, is nader uitgewerkt en gevat in twee tabellen in Bijlage D die gezamenlijk het referentiemodel vormen. In het model is tevens de intentie van een botnet weergegeven, omdat het van belang is de taken en bevoegdheden van de betrokken organisaties te identificeren, ook al is het oogmerk van een botnet meervoudig en meestal niet bij voorbaat duidelijk. De latere wijzigingen en aanvullingen op het theoretisch model naar aanleiding van de empirische onderzoeksgegevens zijn daarbij in rood weergegeven.

Het model voorspelt dat er binnen Nederland een hiaat is ten aanzien van de bevoegdheden voor effectieve botnetbestrijding, omdat benodigde competenties voor botnetbestrijding, gezien de aard van het fenomeen, niet helemaal bij de klassieke taken en bevoegdheden van betrokken overheidsorganisaties passen. Dit hiaat zit met name in het wettelijke verbod om een commandoserver of de communicatie van een botnet over te nemen, het zogenaamde ‘terughacken’. Botnets vormen een robuust geheel en blijven zich ontwikkelen. Ze zijn daarmee een aanhoudende dreiging. De huidige organisatie van botnetbestrijding lijkt daar nog niet volledig effectief tegen opgewassen.

5.2. Conclusies uit het empirisch onderzoek

In het empirisch deel is met een gestructureerd interview op basis van onderzoeksvragen [E.1] tot en met [E.5] een zestal organisaties onderzocht: NCTV, NCSC, OM, politie, DefCERT en Fox-IT. Paragrafen 4.3.1 en 4.3.4 bespreken respectievelijk de uitkomsten van onderzoeksvragen [E.1] en [E.4] die bedoeld zijn om organisaties en hun competenties van het referentiemodel te vergelijken met de werkelijkheid.

5.2.1. **Organisaties**

[E.1] *Welke Nederlandse organisaties bestrijden botnets?*

Het empirisch onderzoek heeft naast de uit het theoretisch onderzoek geïdentificeerde organisaties op basis van [E.1] enkele andere organisaties geïdentificeerd die meer op de achtergrond een rol in botnetbestrijding spelen en niet in het referentiemodel voorkomen: het NFI, SIDN, Ministerie van Economische Zaken en de ACM. Het ontbreken van zulke organisaties hoeft niet als een omissie in het model te worden gezien, omdat het detailniveau van het model beperkt is en alleen de hoofdrolspelers omvat voor wie de betreffende organisaties een specifieke ondersteunende rol vervullen.

5.2.2. **Botnettaxonomie**

[E.2] *Hanteren de organisaties van [E.1] de onder [T.1] en [T.2] geïdentificeerde of vergelijkbare botnettaxonomie en –bestrijdingsmethoden, of hanteren zij een andere benadering?*

Met onderzoeksvraag [E.2] is in Paragraaf 4.3.2 gekeken of de onderzochte organisatie de onder [T.1] en [T.2] geïdentificeerde of vergelijkbare botnettaxonomie en -bestrijdingsmethoden hanteren. Het blijkt dat voor de operationele bestrijding van een botnet een indeling naar enerzijds commandostructuur en anderzijds het oogmerk van het botnet niet relevant is, maar beleidsmatig kan een dergelijke indeling wel de juiste aandacht geven en bijdragen aan een gerichte kennisopbouw bij betrokken organisaties. Voor organisaties is de intentie van een botnet wel leidend om te bepalen of de organisatie dus een rol speelt in de bestrijding ervan. Daarbij is het van belang welke competenties men daarvoor al dan niet zelf (nodig) heeft.

Het deel van het model dat het verband legt tussen botnetstructuur en –intentie enerzijds en bestrijdingsmethode anderzijds, wordt door de onderzochte organisaties niet zo gezien. Hetzelfde geldt voor het verband tussen competenties en bestrijdingsmethoden: ofwel een competentie is ongeacht de bestrijdingsmethode altijd in enige mate relevant, ofwel de competentie is uniek voor de bestrijdingsmethode. Dus Tabel 10 (zie Bijlage D) van het referentiemodel is niet noodzakelijk onjuist, maar het biedt weinig praktische meerwaarde voor de doelstelling van het onderzoek.

5.2.3. **Organisatie en samenwerking**

[E.3] *Op welke wijze zijn de organisaties voor de bestrijding van botnets georganiseerd?*

[E.5] *Voor welke competenties en bevoegdheden werken de betrokken organisaties [E.1] samen met andere organisaties?*

Aan de hand van onderzoeksvragen [E.3]en [E.5] is in Paragraaf 4.3.5 de organisatie en samenwerking onderzocht. Op basis daarvan is het referentiemodel in Bijlage D bijgewerkt. Hierin is te zien over welke competenties en bevoegdheden organisaties gezamenlijk beschikken voor botnetbestrijding in Nederland. Hieruit blijkt een brede samenwerking, met name voor competenties waarbij specifieke kennis van informatietechnologie en botnets nodig is. Wel blijkt dat aan de inlichtingendiensten vooral informatie wordt afgestaan maar slechts beperkt wordt verkregen. De krijgsmacht, uitgezonderd de MIVD, lijkt op dit moment nog geen effectieve speler in het geheel.

Met uitzondering van een aantal wettelijke afhankelijkheden, karakteriseert de samenwerking tussen betrokken organisaties zich door multilaterale samenwerkingsverbanden in fora en werkgroepen, en de inzet van liaisonfunctionarissen. Liaisonfunctionarissen zijn vaste aanspreekpunten voor andere organisaties en dragen zorg voor het uitwisselen van informatie om de samenwerking bij een project of incident te bevorderen. Soms is een liaison van een organisatie fysiek werkzaam binnen een organisatie waarmee wordt samengewerkt. Wederzijds vertrouwen en wederzijdse belangen spelen een grote rol in deze samenwerkingsvormen.

5.2.4. **Bestrijdingsmethoden, bevoegdheden en competenties**

[E.6] *Dekken de Nederlandse organisaties alle aspecten van botnetbestrijding uit het referentiemodel af?*

[E.7] *Welke competenties en bevoegdheden [T.3] hebben en gebruiken de organisaties [E.1], individueel of gezamenlijk, en welke niet?*

[E.8] *Welke geïdentificeerde bestrijdingsmethoden [T.2] worden in de praktijk gebracht, en welke niet?*

In antwoord op onderzoeksvragen [E.6] en [E.8] kan worden geconcludeerd dat Nederlandse organisaties het merendeel van de aspecten van het referentiemodel afdekken, zoals is te zien in Bijlage D. De botnetintentie cyberoorlog en bestrijdingsmethoden en competenties gericht op de fysieke uitschakeling van infrastructuur en/of de botmaster zijn niet onderzocht. Maar op basis van onderzoeksvraag [E.7] is wel duidelijk geworden dat een aantal organisaties individuele en gezamenlijke competenties en bevoegdheden mist. Dat blijkt uit de volgende punten.

Ten eerste zijn competenties om geavanceerde decentrale en hybride botnetstructuren te bestrijden (zoals manipulatie van botagents en communicatie om botnets van binnenuit te verstoren) zeer beperkt aanwezig bij de onderzochte organisaties. Hoewel dergelijke botnets momenteel niet de grootste dreiging lijken te vormen, is niet uitgesloten dat deze competenties binnen afzienbare tijd nodig blijken om effectief botnets te kunnen bestrijden. Met name als de bestrijding van de relatief eenvoudige centraal aangestuurde botnets verbetert, zullen botmasters genoodzaakt zijn zich meer van deze botnetvormen te bedienen.

Ten tweede lijken de overige competenties en bevoegdheden te zijn afgedekt, maar de bevoegdheid tot het aanwenden van essentiële competenties om botnets te analyseren en te bestrijden, beperkt zich voor een belangrijk deel tot het OM en de politie. Deze instanties zijn op hun beurt beperkt in botnetbestrijding omdat enerzijds hun rechtsmacht niet buiten Nederland strekt, en zij anderzijds beperkt zijn in de middelen die zij kunnen aanwenden. Buiten de krijgsmacht en inlichtingendiensten, die niet nader onderzochte bevoegdheden op hun eigen terrein hebben, zijn andere organisaties daarmee in beginsel beperkt tot het detecteren en isoleren van individuele bots en tot het verwijderen van malware. In sommige gevallen kan het botnetverkeer binnen een netwerk worden verstoord met behulp van '*sink holing*'. Zoals uit het literatuuronderzoek is gebleken en in het empirisch onderzoek wordt bevestigd, is een dergelijke aanpak weinig effectief omdat het botnet feitelijk in stand wordt gehouden en de botmaster zijn activiteiten kan blijven ontplooien.

Ten derde is de overheid, voor competenties die gebruik maken van verstoring of manipulatie van de communicatie in een botnet, afhankelijk van kennis, middelen en medewerking van internetaanbieders en grotere partijen die hun eigen netwerken beheren. De medewerking kan in sommige gevallen wel worden afgedwongen.

5.2.5. **Effectiviteit van botnetbestrijding**

[E.9] *Bestaan er daardoor geïdentificeerde soorten botnets [T.1] die niet kunnen worden bestreden?*

Dit betekent, in antwoord op onderzoeksvraag [E.9], dat het OM en de politie met medewerking van computerbeveiligingsbedrijven en internetaanbieders in staat zijn de relatief eenvoudige botnets met een centrale commandostructuur in Nederland en middels rechtshulpverzoeken in het buitenland, effectief te bestrijden. Bovendien kunnen ontdekte botnets worden verstoord door de communicatie ervan te verhinderen, of kunnen bedrijven een '*notice-and-take-down*' (NTD) procedure starten, die de mogelijkheid biedt een klacht ('*notice*') in te dienen op basis waarvan de internetaanbieder kan onderzoeken of er daadwerkelijk sprake is van illegale activiteiten en deze stoppen door een server offline te halen ('*take-down*') (zie Paragraaf 4.3.4.5). Dat neemt echter niet weg dat daarmee niet alle botnets kunnen worden aangepakt en dat het in het bijzonder voor private partijen lastig is zich zelfstandig te verweren tegen met name vanuit het buitenland aangestuurde botnets.

5.2.6. **Verschillen t.a.v. het referentiemodel**

[E.10] *Welke verschillen kunnen worden vastgesteld tussen de wijze waarop de bestrijding van botnets in Nederland is georganiseerd en het referentiemodel voor botnetbestrijding?*

Samenvattend kunnen aan de hand van onderzoeksvraag [E.10] de volgende verschillen worden vastgesteld tussen het referentiemodel voor botnetbestrijding en de wijze waarop de bestrijding van botnets in Nederland is georganiseerd.

- Een harde relatie die het referentiemodel legt tussen 1. de intentie van het botnet, 2. de structuur van het botnet en 3. de bestrijdingsmethode, kan niet worden vastgesteld omdat men die in de praktijk niet zo ervaart.

- Er is een aantal organisaties betrokken bij botnetbestrijding dat niet in het referentiemodel voorkomt; zij spelen meer een (ondersteunende) rol op de achtergrond.

- De NTD-procedure komt niet expliciet in het referentiemodel voor. Deze mogelijkheid zou naast strafrechtelijk beslag, als specifieke vorm van beslaglegging (C13) kunnen worden gezien, namelijk beslaglegging door de hosting provider. Dit is een omissie in het model.

- De competenties 'verstoring met bots' (C8) en 'overnemen communicatie' (C10) zijn niet aanwezig bij de onderzochte organisaties, terwijl op theoretische gronden deze competenties wel waren toegeschreven aan partijen.

5.3. **Discussie**

De kenmerkende uitkomst van het literatuuronderzoek is dat alle organisaties in Nederland door het ontbreken van een bevoegdheid tot terughacken, beperkt zijn in de bestrijding van botnets. Als een botmaster al kan worden opgespoord zonder terughacken, is uitschakeling van een botnet nagenoeg onmogelijk, zeker als het botnet (mede) vanuit het buitenland wordt aangestuurd. Alleen de inlichtingendiensten hebben afdoende bevoegdheden voor het onderzoeken van botnets, maar zij zijn uitsluitend bevoegd om onderzoek te doen en niet om botnets te bestrijden. Uitschakelen van botnets is momenteel theoretisch alleen mogelijk door de krijgsmacht wanneer er sprake is van een gewapend conflict, maar zelfs op dat gebied zijn de capaciteiten van de krijgsmacht en de juridische aspecten niet helder.

Met de aanpassing van het theoretisch referentiemodel op basis van de empirische onderzoeksgegevens, blijven de conclusies van het literatuuronderzoek grotendeels staan. Het onderzoek bevestigt dat effectieve botnetbestrijding lastig is. De betrokken organisaties hebben in beginsel gezamenlijk de competenties in huis een relatief eenvoudig botnet in Nederland effectief aan te pakken, zowel door strafrechtelijke opsporing als door het verstoren van de communicatie. Maar de meest effectieve methoden om botnets te onderzoeken of te bestrijden vraagt ten minste enige vorm van terughacken of aftappen van informatie, terwijl de Nederlandse wetgeving dat verbiedt. Het is daarom nog onvoldoende zeker dat de huidige organisatie in staat is alle botnets afdoende te betstrijden, met name de kleinere, onopvallende en vanuit het buitenland aangestuurde botnets.

Toch zijn er wel enkele nuances aan te brengen. Het OM en de politie maken, ondanks het terughackverbod, in het belang van de openbare orde zelf wel (proportioneel) gebruik van genoemde methoden om effectief te kunnen optreden. Dat blijkt onder meer uit de succesvolle bestrijding van botnets als Bredolab en Pobelka. Onbekend is echter hoeveel botnets daadwerkelijk bekend zijn en hoeveel daarvan niet succesvol kunnen worden bestreden. Bovendien blijken niet alleen dergelijke technologische methoden maar vooral nog klassieke opsporingsmethoden een doorslaggevende rol te spelen om de botmaster en/of opdrachtgevers te achterhalen. De overheid is daarbij wel afhankelijk van de kennis en capaciteit van computerbeveiligingsbedrijven, en de medewerking van internetaanbieders en vitale bedrijven. Er zijn daarom allerlei samenwerkingsvormen op het gebied van botnetbestrijding ontstaan, vaak in de vorm van liaisonfunctionarissen en (inter)nationale fora. Met name het NCSC speelt een belangrijke coördinerende en informatieverstrekkende rol in die samenwerkingsverbanden. Ondanks de samenwerking is de insteek van het OM dat het terughackverbod gehandhaafd blijft en dat de overheid, analoog aan het geweldsmonopolie, het alleenrecht heeft om essentiële competenties voor botnetbestrijding aan te wenden.

Het is essentieel dat de overheid dat monopolie ook weet waar te maken, omdat de publiek-private samenwerking hoofdzakelijk op wederzijdse belangen en wederzijds vertrouwen is gebaseerd. Anders verliest de overheid het vertrouwen en zien de private partijen hun belangen onvoldoende behartigd, met als gevolg dat de noodzakelijke samenwerking onder druk komt te staan. De vraag is of de overheid daarvoor voldoende kennis en middelen kan aanwenden. De overheid is namelijk afhankelijk van internetaanbieders, computerbeveiligingsbedrijven en vitale bedrijven, die, ondanks onvoldoende

bevoegdheden voor de meest essentiële competenties, wel over (andere) belangrijke competenties voor botnetbestrijding beschikken. De verwachting is bovendien dat botnets technologische groei zullen blijven doormaken, juist als bestrijding van de hedendaagse botnets steeds effectiever wordt; het belang en de effectiviteit van traditionele opsporingsmethoden nemen dan af.

Enerzijds ontbreekt dus een aantal competenties dat nodig is voor de bestrijding van complexere botnets. Anderzijds kan een aantal essentiële competenties voor de bestrijding van botnets alleen door de overheid, met beperkte capaciteit en rechtsmacht, worden aangewend. Bovendien is het de vraag of de huidige noodzakelijke samenwerkingsverbanden tussen de overheid en private partijen houdbaar zijn voor de langere termijn. In antwoord op de hoofdvraag kan daarom worden gesteld dat de botnetbestrijding organisatorisch nog niet volledig effectief is ingericht in Nederland.

Het is dan ook aan te raden dat er over alternatieve beleidslijnen wordt nagedacht waarbij onder bepaalde omstandigheden en voorwaarden een private partij 'digitale zelfverdediging' kan toepassen. Een andere mogelijkheid kan liggen in een door de overheid opgezet en aangestuurd operationeel raamwerk voor *cyber defence*. Binnen zo'n structuur kan beleidsafstemming, kennisdeling, gestandaardiseerde informatievoorziening en signalering plaatsvinden. Ook kunnen een duidelijke rolverdeling en richtlijnen worden ontwikkeld welke organisatie, afhankelijk van aard en intentie van het botnet, de primaire bestrijder is. Coördinatie en kennisdeling kunnen op die wijze sneller en efficiënter dan met de huidige bi- en multilaterale verbanden. Deelname van overheidsinstanties, internetaanbieders en vitale bedrijven kan dan niet meer vrijblijvend zijn, maar een dergelijk raamwerk zou wel een garantie moeten bieden voor een open internet zonder meer overheidsregulering dan nodig om cyberdreigingen tegen te gaan.

5.4. Aanbevelingen voor verder onderzoek

Op basis van de conclusies ten aanzien van de botnettaxonomie in Paragraaf 5.2.2 wordt aanbevolen om de relaties tussen de verschillende dimensies te onderzoeken aan de hand van statistische gegevens van bekende botnets en case studies van neergehaalde botnets. Onderzoek of er een correlatie bestaat tussen het oogmerk van een botnet en de complexiteit van een botnet; met andere woorden:

[A.1] Neemt, naarmate een botnet (mede) wordt gebruikt voor meer ernstiger delicten in het gepresenteerde spectrum (Tabel 1), ook de complexiteit van de (commando)structuur van het botnet toe?

Ten aanzien van de conclusie over de effectiviteit van botnetbestrijding in Paragraaf 5.2.5 wordt aanbevolen de mogelijkheden tot digitale zelfverdediging te onderzoeken aan de hand van de volgende onderzoeksvraag:

[A.2] Onder welke voorwaarden is digitale zelfverdediging, binnen en buiten de voorgestelde samenwerkingsstructuur, door private organisaties mogelijk dan wel gewenst, waarbij de aanwending van middelen die momenteel nog bij wet verboden zijn, niet bij voorbaat wordt uitgesloten om effectieve botnetbestrijding mogelijk te maken?

Op basis van de conclusies in Paragraaf 5.2.3 en 5.2.4 en de algemene discussie op het gebied van organisatie en bestrijdingsmethoden, worden de volgende aanbevelingen voor verder onderzoek gedaan:

[A.3] Hoeveel botnets zijn er in Nederland actief (geweest) en hoeveel daarvan zijn of kunnen effectief worden bestreden?

[A.4] Welke belangen prevaleren bij botnetbestrijding, gezien de verschillende taken en mogelijk elkaar tegenwerkende competenties; heeft bijvoorbeeld de opsporing van de dader in alle gevallen een hogere prioriteit dan herstel van een normale situatie (of andersom), wanneer vitale voorzieningen worden getroffen door een botnetaanval?

[A.5] Kan de overheid in de (nabije) toekomst beschikken over voldoende kennis en middelen om het monopolie op essentiële competenties en bevoegdheden voor botnetbestrijding te behouden?

[A.6] Hoe kan het gepresenteerde referentiemodel worden vertaald naar een operationele richtlijn voor de verdeling van taken, bevoegdheden en verantwoordlijkheden van publieke en private organisaties op basis waarvan botnets effectief kunnen worden bestreden?

[A.7] In hoeverre kan een dergelijke richtlijn de basis vormen voor een samenwerkingsstructuur waarbinnen betrokken partijen structureel samenwerken op het gebied van beleidsafstemming, strategische kennisdeling, signalering van botnets en operationele informatie-uitwisseling voor de botnetbestrijding?

De conclusies in Paragrafen 5.2.1 en 5.2.6 leiden niet tot specifieke aanbevelingen voor verder onderzoek.

5.5. Reflectie op het onderzoek

In Hoofdstuk 2 is de onderzoeksmethode verantwoord en wordt gereflecteerd op de validiteit en betrouwbaarheid van de onderzoeksresultaten. Maar zoals ieder onderzoek kende ook dit afstudeertraject in verschillende fasen de nodige afwegingen en leermomenten. Ter afsluiting van dit rapport is het zinvol om op een aantal van deze aspecten kort terug te blikken.

De genomen moeite en tijd om in de fasen van formulering van de onderzoeksopdracht en -aanpak een duidelijke en uitvoerbare probleemstelling te definiëren, is welbesteed geweest. In de literatuurstudie en de interviewgesprekken had ik regelmatig de neiging om breder en dieper op het onderwerp in te gaan, of om een ander perspectief aan te nemen en het fenomeen botnets in andere contexten (zoals juridische kaders, raamwerken voor computerbeveiliging, etc.) te bezien. Maar de doelstelling en onderzoeksvragen zorgden voor gerichte voortgang. Met name de keuze om het organisatorische aspect van botnetbestrijding vanuit een discreet aantal bevoegdheden en competenties te benaderen, heeft hieraan bijgedragen. De scope van het onderzoek is telkens kritisch bekeken, waar nodig aangescherpt, maar is gedurende het onderzoek niet aangepast hoeven worden.

Het grootste obstakel in het onderzoek was toegang krijgen tot de te onderzoeken organisaties. Hoewel ik mij vooraf bewust was van het feit dat het enige inspanning vraagt om bij verschillende organisaties de juiste personen te vinden en hen te overtuigen van de meerwaarde van deelname aan een onderzoek, viel dit aspect mij toch tegen. Antwoorden lieten soms weken op zich wachten en enkele afspraken moesten worden verzet, waardoor het aanzienlijk meer tijd kostte om voldoende deelname zeker te stellen.

Uiteindelijk heeft de afronding van het eindrapport ruim anderhalve maand langer geduurd dan ik had gepland. Dat het onderzoek niet in de beschikbare tijd zou kunnen worden afgerond, was voor mij echter een minder groot risico dan dat er te weinig organisaties konden worden onderzocht zodat de onderzoeksopdracht en/of -aanpak zou moeten worden bijgesteld. De vraag rees of bijvoorbeeld een enquête onder een groter aantal organisaties, niet praktischer zou zijn geweest. Maar gezien het specialistische en gevoelige karakter, is de keuze voor interviews bij nader inzien toch juist gebleken. Tijdens de interviews merkte ik ook dat de onderzochte organisaties en geïnterviewden de verschillende aspecten van botnetbestrijding anders ervaren of er op basis van hun rol een ander gewicht aan toekennen. Met een enquête was dit wellicht niet duidelijk geworden, terwijl ik met de interviews hier juist op heb kunnen inspelen.

Het afstudeertraject heeft het resultaat opgeleverd dat ik voor ogen had. Het onderzoek heeft mij actuele kennis en inzicht verschaft over een fascinerend onderwerp als botnetbestrijding en ik heb kunnen leren hoe anderen in diverse organisaties omgaan met de uitdagingen waar zij zich voor geplaatst zien. Maar ik heb mij in een wetenschappelijke context vooral verder kunnen bekwamen in het analyseren en formuleren van een probleem, evenals in het zoeken naar de juiste en relevante informatie in de literatuur en in de praktijk, om op basis van kritische analyse en met waardevolle terugkoppeling van mijn begeleider te komen tot onderbouwde conclusies en aanbevelingen.

Referenties

1. Wetenschappelijke literatuur

Aviv, A. J., & Haeberlen, A. (2011). Challenges in experimenting with botnet detection systems. *USENIX 4th CSET Workshop*, San Francisco, CA. Retrieved December 23, 2012, from http://static.usenix.org/event/cset11/tech/final_files/Aviv.pdf

Bleaken, D. (2010). Botwars: the fight against criminal cyber networks. *Computer Fraud & Security*, 2010(5), 17–19. Retrieved December 29, 2012, from http://www.sciencedirect.com/science/article/pii/S1361372310700555

Chapman, I. M., Leblanc, S. P., & Partington, A. (2011). Taxonomy of cyber attacks and simulation of their effects. *Proceedings of the 2011 Military Modeling & Simulation Symposium* (pp. 73–80). Retrieved October 31, 2012, from http://dl.acm.org/citation.cfm?id=2048569

Clark, D. D., & Landau, S. (2010). The problem isn't attribution: it's multi-stage attacks. *Proceedings of the Re-Architecting the Internet Workshop* (p. 11). Retrieved December 24, 2012, from http://dl.acm.org/citation.cfm?id=1921233.1921247

Czosseck, C. G. (2012). *An Evaluation of State-Level Strategies Against Botnets in the Context of Cyber Conflicts.* Estonian Business School, Tallinn.

Dagon, D., Gu, G., Lee, C. P., & Lee, W. (2007). A taxonomy of botnet structures. *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual* (pp. 325–339). Retrieved October 24, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4413000

Ducheine, P. A. L., & Voetelink, J. E. D. (2011). Cyberoperaties: naar een juridisch raamwerk. *Militaire Spectator*, 180(6), 273–286.

Eeten, M. J. G. van, Asghari, H., Bauer, J. M., & Tabatabaie, S. (2011). *ISPs and Botnet Mitigations: A Fact-Finding Study on the Dutch Market*. TU Delft.

Estrada, V. C., & Nakao, A. (2010). A Survey on the Use of Traffic Traces to Battle Internet Threats. *Knowledge Discovery and Data Mining, 2010. WKDD'10. Third International Conference on* (pp. 601–604). Retrieved December 23, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5432468

Fedynyshyn, G., Chuah, M. C., & Tan, G. (2011). Detection and Classification of Different Botnet C&C Channels. In J. M. A. Calero, L. T. Yang, F. G. Mármol, L. J. García Villalba, A. X. Li, & Y. Wang (Eds.), *Autonomic and Trusted Computing* (Vol. 6906, pp. 228–242). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved November 23, 2012, from http://www.springerlink.com/index/10.1007/978-3-642-23496-5_17

Feily, M., Shahrestani, A., & Ramadass, S. (2009). A survey of botnet and botnet detection. *Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on* (pp. 268–273). Retrieved December 23, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5210988

Hunt, R., & Slay, J. (2010). The Design of Real-Time Adaptive Forensically Sound Secure Critical Infrastructure. *Network and System Security (NSS), 2010 4th International Conference on* (pp. 328–333). Retrieved December 29, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5635616

Koning, M. E. (2011, September). *Terughacken als opsporingsmethode: een juridische analyse van de terughack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling.* Universiteit van Amsterdam, Amsterdam. Retrieved from http://www.bredolab.nl/wp-content/uploads/2011/11/Terughacken-als-opsporingsmethode-scriptie-Merel-Koning-september-2011.pdf

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging*

Transdiscipline, 9, 181–212. Retrieved October 24, 2012, from http://www.scs.ryerson.ca/aferworn/courses/CP8101/CLASSES/ConductingLiteratureReview.pdf

Li, C., Jiang, W., & Zou, X. (2009). Botnet: Survey and case study. *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on* (pp. 1184–1187). Retrieved November 7, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5412718

Lin, W., & Lee, D. (2012). Traceback Attacks in Cloud–Pebbletrace Botnet. *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on* (pp. 417–426). Retrieved December 27, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6258188

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. *EURASIP Journal on Wireless Communications and Networking*, 2009(1), 692654. Retrieved October 24, 2012, from http://jwcn.eurasipjournals.com/content/2009/1/692654

Liu, S., Gong, J., Yang, W., & Jakalan, A. (2011). A Survey of Botnet Size Measurement. *Networking and Distributed Computing (ICNDC), 2011 Second International Conference on* (pp. 36–40). Retrieved December 23, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6047102

Lodder, A. R., & Boer, L. J. M. (2012). Cyberwar? What war? *Justitiële verkenningen: veiligheid in cyberspace*, 38(1), 52–66.

Lu, T. T., Liao, H. Y., & Chen, M. F. (2011). An Advanced Hybrid P2P Botnet 2.0. *World Academy of Science, Engineering and Technology,* (57), 595–597. Retrieved November 22, 2012, from http://www.waset.ac.nz/journals/waset/v57/v57-115.pdf

Mendonça, L., & Santos, H. (2012). Botnets: A Heuristic-Based Detection Framework (pp. 33–40). ACM Press. Retrieved November 19, 2012, from http://dl.acm.org/citation.cfm?doid=2388576.2388580

Patil, S. P., & Kumar, S. (2011). Botnet: A Network Threat. *International Journal of Computer Applications Proceedings on International Conference on Recent Trends in Information Technology and Computer Science.* Retrieved from http://www.ijcaonline.org/archives/icrtitcs/number1/5174-1006

Paxton, N. C., Ahn, G., & Shehab, M. (2011). MasterBlaster: Identifying Influential Players in Botnet Transactions. Computer Software and Applications Conference (COMPSAC), 2011 IEEE 35th Annual (pp. 413–419). Retrieved December 23, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6032373

Puri, R. (2003). *Bots & botnet: An overview*. SANS Institute 2003. Retrieved November 19, 2012, from http://home.engineering.iastate.edu/~guan/course/CprE-536/paperreadinglist606/botnet-overview.pdf

Raghava, N. S., Sahgal, D., & Chandna, S. (2012). Classification of Botnet Detection Based on Botnet Architechture. *Communication Systems and Network Technologies (CSNT), 2012 International Conference on* (pp. 569–572). Retrieved December 7, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6200734

Rajab, M. A., Jay Zarfoss, Fabian Monrose, & Andreas Terzis. (2007). My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging. Proc. of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots 2007). Retrieved October 31, 2012, from http://www.usenix.org/event/hotbots07/tech/full_papers/rajab/rajab.pdf

Rajab, M. A., Zarfoss, J., Terzis, A., & Monrose, F. (2006). A multifaceted approach to understanding the botnet phenomenon. *Proceedings of the 2006 ACM SIGCOMM Internet Measurement Conference (IMC)* (Vol. 2006). Retrieved October 24, 2012, from http://hinrg.cs.jhu.edu/joomla/uploads/Main/IMC06.pdf

Saunders, M., Lewis, P., Thornhill, A., Verckens, J. P., & Smitt, P. (2011). *Methoden en technieken van onderzoek*. Amsterdam: Pearson Education.

Stol, W. P., Leukfeldt, E. R., & Klap, H. (2012). Cybercrime en politie. Justitiële verkenningen: veiligheid in cyberspace, 38(1), 25–39.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., et al. (2009). Your botnet is my botnet: analysis of a botnet takeover. *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 635–647). Retrieved November 7, 2012, from http://dl.acm.org/citation.cfm?id=1653738

Tettero, M.A.D., & P. de Graaf. (2010) "Het Vijfde Domein Voor de Krijgsmacht: Naar Een Integrale Strategie Voor Digitale Defensie." *Militaire Spectator* 179, no. 5: 240–248.

Tyagi, A. K., & Aghila, G. (2011). A Wide Scale Survey on Botnet. *International Journal of Computer Applications*, 34(9). Retrieved November 20, 2012, from http://research.ijcaonline.org/volume34/number9/pxc3875948.pdf

Vogt, R., Aycock, J., & Jacobson, M. (2007). Army of botnets. *Proceedings of the 2007 Network and Distributed System Security Symposium (NDSS 2007)* (pp. 111–123). Retrieved October 31, 2012, from https://www.isoc.org/isoc/conferences/ndss/07/papers/army_of_botnets.pdf

Wang, P., Aslam, B., & Zou, C. C. (2010). Peer-to-Peer Botnets: The Next Generation of Botnet Attacks. *Electrical Engineering*, 1–25. Retrieved October 31, 2012, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.153.6675&rep=rep1&type=pdf

Wang, P., Sparks, S., & Zou, C. C. (2010). An advanced hybrid peer-to-peer botnet. *Dependable and Secure Computing, IEEE Transactions on*, 7(2), 113–127. Retrieved November 22, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4569852

Xiang, C., Binxing, F., Peng, L., & Chaoge, L. (2012). Advanced triple-channel botnets. *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 1019–1021). ACM Press. Retrieved November 7, 2012, from http://dl.acm.org/citation.cfm?doid=2382196.2382311

Yu, S., Zhou, W., Dou, W., & Makki, S. K. (2012). Why it is Hard to Fight against Cyber Criminals? *Distributed Computing Systems Workshops* (ICDCSW), 2012 32nd International Conference on (pp. 537–541). Retrieved December 23, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6258202

Zhang, L., Yu, S., Wu, D., & Watters, P. (2011). A survey on latest botnet attack and defense. *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on* (pp. 53–60). Retrieved December 7, 2012, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6120803

Zhu, Z., Lu, G., Chen, Y., Fu, Z. J., Roberts, P., & Han, K. (2008). Botnet Research Survey (pp. 967–972). IEEE. Retrieved October 31, 2012, from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4591703

2. Niet-wetenschappelijke bronnen

Cybersecuritybeeld Nederland 2013. (2013). Nationaal Cyber Security Centrum. Retrieved from http://www.nctv.nl/Images/ncscscbn-3nl-pp-03_tcm126-504698.pdf

Eijk, L. van der. (22 april 2013). Onderzoeksinterview met DefCERT.

Grondwet voor het Koninkrijk der Nederlanden. (n.d.). Retrieved from http://wetten.overheid.nl/BWBR0001840

Factsheet Notice-and-Take-Down. (n.d.). ICTRecht. Retrieved from https://ictrecht.nl/factsheets/notice-and-takedown/

High Tech Crime: Criminaliteitsbeeldanalyse 2012. (2012, March). Korps Landelijke Politie Diensten.

Kennisdocument Taurus. (2011, March). Korps Landelijke Politie Diensten.

Koops, B.-J. (2013). *Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: strafrechtelijke aspecten*. Retrieved May 23, 2013, from http://www.surfnet.nl/documents/expert%20opinion%20mei%202013-1.pdf

Maas, T., Bernaards, F., Wagenaar, P., & Graaf, D. de. (23 april 2013). Onderzoeksinterview met Team High Tech Crime van de Politie.

Minister van Justitie. (15 oktober 2012). *Wetgeving bestrijding cybercrime*. Retrieved January 6, 2013, from https://zoek.officielebekendmakingen.nl/kst-28684-363.pdf

Nadere analyse Pobelka-botnet. (2013). Nationaal Cyber Security Centrum. Retrieved from http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/04/04/onderzoek-pobelka-botnet/lp-v-j-0000003002.pdf

OM Jaarbericht 2012. (mei 2013). Openbaar Ministerie. Retrieved May 6, 2013, from http://www.jaarberichtom.nl/

Opsporingsbevoegdheid opsporingsambtenaren Koninklijke marechaussee. (2010). Parket bij de Hoge Raad. Retrieved from http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2010:BK6142.

Organisatieregeling Ministerie van Veiligheid en Justitie 2011. (2011). Retrieved from http://wetten.overheid.nl/

Politiewet 2012. (2012). Retrieved from wetten.overheid.nl/BWBR0031788

Prins, R. (2012). Een veilige cyberwereld vraagt nieuw denken. Justitiële verkenningen: veiligheid in cyberspace, 38(1), 40–51. Retrieved December 31, 2012, from https://www.wodc.nl/onderzoeksdatabase/jv201201-veiligheid-in-cyberspace.aspx

Prins, R. (23 mei 2013). Onderzoeksinterview met Fox-IT.

Sande, J. van de, Woutersen, D., & Leeuwen, M. van. (2013, October 6). Interview met NCTV / NCSC.

Taxonomy of Botnet Threats. (2006). Trend Micro Inc. Retrieved from http://www.cs.ucsb.edu/~kemm/courses/cs595G/TM06.pdf

Weggeman, M. (1997). *Kennismanagement, inrichting en besturing van kennisintensieve organisaties.* Schiedam: Scriptum Management.

Wet op de inlichtingen- en veiligheidsdiensten 2002. (2002). Retrieved from http://wetten.overheid.nl/BWBR0013409

Wet op de rechterlijke organisatie. (n.d.). Retrieved from http://wetten.overheid.nl/BWBR0001830

Wetboek van Strafrecht. (n.d.). Retrieved from http://wetten.overheid.nl/BWBR0001854

Wetboek van Strafvordering. (n.d.). Retrieved from http://wetten.overheid.nl/BWBR0001903/

Zwieten, L. van. (6 mei 2013). Onderzoeksinterview met het OM.

Bijlage A. Fasering van het onderzoekstraject

1. Voorlopige opdrachtformulering

Formuleren van een vraagstelling over een relevant onderzoeksonderwerp, het uitwerken ervan in een opdrachtformulering en een bijbehorend voorlopig plan van aanpak. Dit wordt verwoord in het Rapport *Voorlopige Opdrachtformulering*, waarin de nadruk zal liggen op de gekozen vraagstelling (onderzoeksvragen) en de opzet van de literatuurstudie.

2. Literatuurstudie

De literatuurstudie is gericht op het beantwoorden van de in de voorlopige opdrachtformulering gestelde onderzoeksvragen. Het resultaat hiervan is een conceptueel model of een referentiemodel, dat als uitgangspunt kan dienen bij de opzet van een empirische toetsing. Dit wordt vastgelegd in het Rapport *Literatuurstudie*

3. Aanscherping opdrachtformulering

Definiëren van een definitieve onderzoeksopdracht op basis van de literatuurstudie. Het Rapport *Definitieve Opdrachtformulering* bevat een concrete onderzoeksdoelstelling met bijbehorende empirische onderzoeksvragen (onderzoekbare probleemstelling) voor de empirische toetsing van het conceptueel model of referentiemodel.

4. Formulering onderzoeksaanpak

Ontwikkelen van een passende, gedetailleerde onderzoeksaanpak. Het Rapport *Onderzoeksaanpak* beschrijft en verantwoordt hoe de gekozen methoden en technieken leiden tot beantwoording van de empirische onderzoeksvragen afgeleid uit de probleemstelling.

5. Uitvoering empirisch onderzoek

Uitvoeren van de gekozen onderzoeksaanpak door:

- gegevensverzameling: bestaand of nieuw materiaal leveren de resultaten van het onderzoek;
- analyse (kwantitatief of kwalitatief) van de resultaten als antwoord op de onderzoeksvragen;
- het trekken van conclusies: confrontatie van de resultaten in het licht van de onderzoeksvragen;
- het formuleren van aanbevelingen voor vervolgonderzoek, in de vorm van nieuwe onderzoeksvragen.

6. Rapportage

Het schrijven van het afstudeerverslag / eindrapport op basis van de resultaten en rapporten van de vorige fasen.

7. Presentatie en verdediging

Verzorgen van een openbare presentatie van het onderzoek voor de begeleidingscommissie en enkele collega-afstudeerders, gevolgd door een besloten verdediging van het resultaat.

Bijlage B. Lijst van Contacten

1. Begeleiders

Open Universiteit, Faculteit Informatica:

- Dhr. dr.ir. Harald Vranken, 1e begeleider en examinator
- Dhr. dr.ir. Arjan Kok en mw. dr. Anda Counotte-Potman, 2e begeleiders

2. Geïnterviewden

Directie Cyber Security:

- Dhr. drs. Michel van Leeuwen, hoofd beleidscluster

2.1. Nationaal Cyber Security Centrum (NCSC)

Afdeling Ontwikkeling & Programma's:

- Dhr. Justus van der Sande, beleidsadviseur

Afdeling Monitoring & Respons:

- Dhr. Dave Woutersen, security specialist

2.2. Openbaar Ministerie

Landelijk Parket:

- Dhr. mr. L.J.A. (Lodewijk) van Zwieten, landelijk Officier van Justitie voor cybercrime

2.3. Politie

Team High Tech Crime van de Nationale Recherche:

- Dhr. ing. Ton Maas, coördinator
- Dhr. Frank Bernaards LL.M., beleidsadviseur
- Dhr. Peter Wagenaar, digitaal rechercheur
- Dhr. Daan de Graaf, digitaal rechercheur

2.4. Defensie

Defensie Computer Emergency Response Team (DefCERT):

- Dhr. Leon van der Eijk, senior analist

2.5. Privaat computerbeveiligingsbedrijf

Fox-IT:

- Dhr. Ronald Prins, directeur - oprichter.

Bijlage C. Literatuurselectie

Het zoeken naar literatuur voor de eerste twee onderzoeksvragen [T.1] en [T.2] is voornamelijk gebeurd via internet door gebruik te maken van de zoekfuncties van de Open Universiteit, ACM Digital Library, IEEE Digital Library en Google Scholar. Twee gebruikte artikelen uit de Militaire Spectator waren mij al bekend.

Tabel 9. Overzicht van gevonden literatuur per onderzoeksvraag

Onderzoeks-vraag	Zoektermen	ACM	IEEE	Google Scholar	Gescand	Bestudeerd	Geciteerd
[T.1]	botnet	578	771	9700	70	29	30
	~ definition	210	113	3.560			
	~ characteristics	292	184	4.000			
	~ taxonomy	72	61	1.170			
[T.2]	~ detection	461	496	6.700	30*	21	
	~ tracking	209	191	4.190			
	~ metrics	201	99	2.240			
	~ analysis	507	442	6970			
	botmaster traceback	4	5	153			
	internet traceback	258	307	16.200			
	botnet takeover	34	25	821			
	~ takedown	20	14	781			

* In aanvulling op de eerste onderzoeksvraag

Bij de selectie van de gevonden artikelen is primair uitgegaan van de relevantie die door de zoekmachine in de sortering is gebruikt. Vervolgens zijn op basis van titel en samenvatting 100 artikelen gescand om te zien welke het beste aansloten bij de onderzoeksvragen en subvragen. Daarnaast zijn 15 artikelen als referentie van een andere bron opgezocht. Bij selectie van de te gebruiken literatuur ging de voorkeur uit naar:

- recente artikelen (van na 2009) die de eigenschappen en bestrijding van botnets op basis van andere, specifieke onderzoeken zo volledig mogelijk in kaart brachten (surveys en meta-onderzoeken);
- bronnen die bij meerdere zoekopdrachten tussen de resultaten voorkwamen;
- bronnen die vaker werden geciteerd (door andere gevonden bronnen); en
- bronnen die een tegenspraak bevatten met een andere bron.

Daar waar oudere artikelen of artikelen die specifiekere aspecten behandelen een aanvulling of verduidelijking brachten, zijn enkele daarvan ook gebruikt. Niet primair als onderzoeksbron, maar voor aansluiting bij de (maatschappelijke) context zijn bij het onderzoek ongeveer vijf niet-wetenschappelijke rapporten van de overheid geraadpleegd.

Om uit het geheel van relevante bronnen een toereikende subset te selecteren, zijn 29 bronnen bestudeerd voor de eerste onderzoeksvraag, en 21 aanvullende bronnen voor de tweede onderzoeksvraag. Uiteindelijk zijn er daarvan 30 geciteerd en opgenomen in de literatuurlijst; niet geciteerde bronnen brachten geen aanvullende informatie of nieuwe inzichten.

Zoekacties voor literatuur over competentie ten aanzien van botnetbestrijding gaven geen resultaat. Voor onderzoeksvragen [T.3] en [T.4] is daarom op de eerste plaats gebruik gemaakt van de uitkomsten en literatuurbronnen van onderzoeksvraag [T.2]. Daarbij zijn openbare bronnen op websites van de Nederlandse overheid gezocht. Naast enkele rapporten zijn een viertal relevante artikelen uit een recent themanummer over veiligheid in cyberspace van het tijdschrift Justitiële Verkenningen van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Veiligheid en Justitie bestudeerd, evenals enkele referenties daaruit. Tot slot zijn zeven wetboeken gebruikt voor naslag aangaande bevoegdheden binnen Nederland.

Bijlage D. Referentiemodel

Tabel 10. Overzicht van bestrijdingsmethoden, commandostructuur en benodigde competenties, bijgewerkt aan de hand van empirische onderzoeksgegevens

Aangrijpingspunt	Bots	Botnetstructuur			Botmaster	
Bestrijdingsmethode	Verwijderen bots uit het botnet	Overname of uitschakelen commandoserver(s)	Verstoring van het botnet met gemanipuleerde bots.	Overname of verstoring van het botnet door manipulatie van de communicatie	Arresteren en vervolgen van de botmaster(s).	Botmaster(s) en/of opdrachtgevers en/of infrastructuur fysiek uitschakelen.
Commandostructuur						
Centraal	○	●			○	○
Decentraal	○		●	●	○	○
Complex / Hybride	○		●	●	○	○
Intentie van het botnet						
A cybervandalisme	○	○	○	○	●	
B misdaad internet	○	○	○	○	●	
C cybercriminaliteit	○	○	○	○	●	
D hacktivisme	○	○	○	○	●	
E cyberterrorisme	○	○	○	○	●	●
F cyberoorlog	○	○	○	○		●
Competentie						
C1 honeynet detectie	●	●	●	●	●	●
C2 passieve detectie	●	●	●	●	●	●
C3 malware onderzoek	●	●	●	●	●	
C4 botnet onderzoek		●	●	●	●	●
C5 ontcijferen		◎	◎	◎	◎	◎
C6 verwijderen malware	✪					
C7 overnemen server		✪				
C8 verstoring met bots			✪			
C9 verstoren comms				✪		
C10 overnemen comms						
C11 traceren op internet		●		◎	●	●
C12 opsporen botmaster					✪	
C13 beslag / NTD server		✪			◎	
C14 bewijsmateriaal					✪	◎
C15 arresteren botmaster					✪	
C16 opsporing in buitenland						✪
C17 fysiek uitschakelen						✪
C18 onderzoek	○	○	○	○	○	○
C19 coördinatie		○	○	○	○	○

Legenda

✪ Kenmerkende competentie voor de bestrijdingsmethode

● Noodzakelijke competentie voor de bestrijdingsmethode / Bestrijdingsmethode is meest passend voor commandostructuur of oogmerk

◎ Afhankelijk van de omstandigheden meer of minder noodzakelijke competentie

○ Bestrijdingsmethode is relevant voor alle commandostructuren of intenties / Algemene competentie; niet gerelateerd aan de bestrijdingsmethode

De rode symbolen geven aanpassing van het referentiemodel n.a.v. empirisch onderzoek aan

Tabel 11. Overzicht van organisaties met competenties en bevoegdheden voor botnetbestrijding, bijgewerkt aan de hand van empirische onderzoeksgegevens

	NCTV	AIVD	OM	Politie	MIVD	Krijgsmacht	Internet-aanbieder	Computer-beveiligingsbedrijf	Vitaal bedrijf	Niet-vitaal bedrijf / particulier	Universiteiten / Hogescholen
Botnet intentie											
A cybervandalisme			●	●		❶ ●	●	●	○	○	
B misdaad internet		◎	●	●		❶ ○	○	●	○	○	
C cybercriminaliteit	●	◎	●	●		❶ ●	●	●	●	○	
D hacktivisme	●	●	●	●	●	❶ ○	○	●	●	○	
E cyberterrorisme	●	●	●	●	●	● ○	○	●	●		
F cyberoorlog	◎	●			●	● ○	○	●	●		
Competentie / bevoegdheid											
C1 honeynet detectie	●/○	●	❸	●	●	❷	○	●	●/○		
C2 passieve detectie	●	●		◎	●	●	●	◎	●	○	
C3 malware onderzoek	●/○	●	❸	●	●	❷		●	●/○		
C4 botnet onderzoek		●	❸	●	●	❷		⊙	○		
C5 ontcijferen		✪	❸	●	✪	❷		⊙			
C6 verwijderen malware		●			●	●	●	◎	●	○	
C7 overnemen server				●		●/❶	○	⊙	○		
C8 verstoring met bots				⊖		●/❶	⊖	⊖	⊖		
C9 verstoren comms	○			⊙		●/❶	●	◎	●		
C10 overnemen comms				⊖		●/❶	⊖	⊖	⊖		
C11 traceren op inet		●	❸	⊙	●	●/❶	●	●/○	●		
C12 opsporen botmast.		●	❸	✪	●	❶/◎		●			
C13 beslag / NTD server	○		❸	✪		❶/◎	●	○	○	○	
C14 bewijsmateriaal	○		❸	✪		❶/◎	◎	◎	◎		
C15 arresteren botmast.			✪	✪		❶/◎					
C16 opsporing buitenl.		◎			◎	❷					
C17 fysiek uitschakelen						✪					
C18 onderzoek	○	○	❹	❹	○	❹	○	●	○		●
C19 coördinatie	●	○	●	●	○	●	○	◎	○		

Legenda

- ● Organisatie is zelfstandig competent of zou het moeten zijn
- ✪ Kerncompetentie van een organisatie en/of exclusieve bevoegdheid
- ◎ Organisatie is competent of zou het moeten zijn, maar handelt alleen in overeenstemming of op gezag
- ⊙ Organisatie is zelfstandig competent of zou het moeten zijn, maar is niet bevoegd
- ○ Organisatie is niet (volledig) zelf competent, maar maakt gebruik van derden

Notities

- ❶ Betreffende bevoegdheid behelst strafbare feiten ten aanzien van de krijgsmacht en berust binnen de krijgsmacht bij de marechaussee die dezelfde bevoegdheden heeft als de politie
- ❷ Voor deze competentie maakt de krijgsmacht gebruik van de MIVD of zet middelen in voor de MIVD
- ❸ Het OM is bevoegd, maar deze taken worden feitelijk door de politie uitgevoerd
- ❹ Justitie en Defensie doen zelfstandig (wetenschappelijk) onderzoek op hun werkterreinen

De rode symbolen geven aanpassing van het referentiemodel n.a.v. empirisch onderzoek aan

Bijlage E. Interviewvragen

1. Inleiding op het interview

1.1. Achtergrond van het interview

Dit interview maakt deel uit van een afstudeeronderzoek aan de Faculteit Informatica van de Open Universiteit Nederland. Het onderzoek richt zich op de botnetbestrijding in Nederland. Een botnet is een zelfverspreidend en zelforganiserend gedistribueerd computerplatform dat gebruik maakt van onvrijwillig geïnfecteerde computers en dat zowel intern als extern zelfstandig cyberaanvallen in opdracht van een persoon of organisatie gecoördineerd kan uitvoeren.

Het Ministerie van Veiligheid & Justitie geeft in de Nationale Cyber Security Strategie het belang aan van gezamenlijk (militair-civiel, publiek-privaat, nationaal-internationaal) optreden tegen cyberdreigingen om schade door misbruik, verstoring of uitval te voorkomen (Ministerie van Veiligheid en Justitie, 2011). Maar het strategisch kader maakt niet inzichtelijk hoe de samenwerking in Nederland op het gebied van cyberveiligheid georganiseerd zou moeten zijn om effectief op te treden tegen concrete dreigingen van botnets. Daarom wordt in dit onderzoek op basis van de specifieke eigenschappen van botnets de organisatie van botnetbestrijding in Nederland onder de loep genomen.

Het doel van het interview is om op systematische wijze te inventariseren over welke competenties en bevoegdheden een organisatie beschikt om verschillende soorten botnets te betstrijden. Na inventarisatie van competenties en bevoegdheden van verschillende organisaties wordt aan de hand van een referentiemodel voor de bestrijding van botnets geanalyseerd of in Nederland de daarvoor benodigde competenties en bevoegdheden zijn afgedekt.

1.2. Opzet van het interview

Het betreft een gestructureerd interview. Dat wil zeggen dat alle geïnterviewden exact dezelfde vragen krijgen. De vragen sluiten aan bij een referentiemodel voor botnetbestrijding. De interviewer zal tijdens het interview de specifieke aspecten uit het referentiemodel waarnaar wordt gevraagd zo nodig toelichten.

In het interview zal eerst een aantal vragen worden gesteld over de geïnterviewden en de organisatie namens wie zij worden geïnterviewd. Vervolgens wordt ingegaan op de soorten botnets die de organisatie onderscheidt en de daarvoor gehanteerde bestrijdingsmethoden. Daarna zal worden gesproken over de competenties en bevoegdheden waarover de organisatie al dan niet zelf beschikt en/of afhankelijk is van andere partijen.

Per organisatie wordt één interview afgenomen. Het interview kan voor een organisatie met meerdere personen tegelijk worden gehouden. De duur van het interview is ongeveer 2 uur.

Het interview wordt niet opgenomen, maar er zullen wel aantekeningen en een verslag worden gemaakt. Het verslag wordt ter goedkeuring aan de geïnterviewden voorgelegd. Gevoelige en vertrouwelijke informatie wordt niet vastgelegd. Indien gewenst wordt het verslag geanonimiseerd of helemaal weggelaten uit het eindrapport. De bevindingen worden uiteraard wel in het eindrapport van het onderzoek verwerkt.

2. Algemene vragen over de organisatie

2.1. Geïnterviewden

Dit deel is bedoeld om algemene informatie over de geïnterviewde(n) te verkrijgen.

Per geïnterviewde:

I.1.1. Wat is uw naam (incl. voorletters, evt. rang en titels)?
I.1.2. Tot welke organisatie behoort u?
I.1.3. Wat is uw functie / relatie tot botnetbestrijding?

2.2. Organisatie

Dit deel is bedoeld om algemene informatie over de organisatie te verkrijgen.

I.2. Wat is de volledige naam van de organisatie? Wordt dit afgekort of zijn er andere aanduidingen voor de organisatie?
I.3. Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?
I.4. Indien van toepassing: wat is de rechtsbasis waaraan de organisatie haar bestaan en taken ontleent?
I.5. Zijn er relevante openbare publicaties, zoals rapporten en jaarverslagen, van en over uw organisatie beschikbaar waarin cyber security in het algemeen of botnetbestrijding in het bijzonder aan de orde komen?

2.3. Andere organisaties

De volgende interviewvragen zijn bedoeld om gegevens te verzamelen om onderzoeksvraag [E.1] te kunnen beantwoorden.

I.6. Welke andere organisaties die zich bezighouden met botnetbestrijding in Nederland zijn u bekend?

Per bekende organisatie:

I.6.1. Wat is de naam van die organisatie?
I.6.2. Wat voor soort organisatie betreft het?
I.6.3. Publieke organisatie?
I.6.4. Private organisatie: internetaanbieder / beveiligingsbedrijf / vitaal bedrijf / anders?
I.6.5. Werkt u ook samen met die organisatie? Ad hoc of structureel?

I.7. Met welke internationale organisaties werkt u samen?

3. Botnetclassificatie en -bestrijdingsmethoden

Om te bepalen in hoeverre men in de praktijk op eenzelfde wijze als in het referentiemodel naar botnetbestrijding kijkt, wordt gekeken welke botnetclassificatie en -bestrijdingsmethoden door betreffende organisaties worden gehanteerd. Deze gegevens zijn bedoeld om onderzoeksvraag [E.2] te kunnen beantwoorden.

3.1. Botnetclassificatie

Op basis van onderzoeksvraag [T.1] hanteert het referentiemodel een taxonomie op basis van intentie en commandostructuur. De volgende interviewvragen dienen om te beoordelen of de organisatie een (soort)gelijke indeling hanteert.

I.8. Gebruikt uw organisatie een indeling, classificatie of taxonomie om verschillende soorten botnets te onderscheiden?

I.9. Zo ja, is dit een indeling, classificatie of taxonomie gebaseerd op:
   a. de intentie van het botnet?
   b. de commandostructuur van het botnet?

Indien één van bovenstaande indelingen wordt gehanteerd, per indeling:

I.9.1. Komt de gehanteerde indeling overeen met de taxonomie van het referentiemodel? Waar zitten de verschillen?

De interviewer zal de botnettaxonomie toelichten en aan de hand van de antwoorden doorvragen.

Indien een andere indeling, classificatie of taxonomie wordt gehanteerd:

I.9.2. Wat voor botnetindeling, -classificatie of -taxonomie hanteert uw organisatie?

I.9.3. Wat zijn de redenen om voor een dergelijke indeling te kiezen?

3.2. Botnetbestrijdingsmethoden

Op basis van onderzoeksvraag [T.2] hanteert het referentiemodel een indeling van bestrijdingsmethoden.

I.10. Op welke wijze of met welke methoden bestrijdt uw organisatie botnets? Met andere woorden: hoe gaat uw organisatie te werk?

Per bestrijdingsmethode:

I.10.1. Bij wat voor soort botnets (conform de besproken classificatie) past u deze bestrijdingsmethode toe?

I.10.2. Richt deze methode zich (primair) op individuele bots, de structuur van het botnet of tegen de botmaster?

I.10.3. Komen de gehanteerde bestrijdingsmethoden overeen met de methoden in het referentiemodel? Waar zitten de verschillen?

De interviewer zal de bestrijdingsmethoden die het referentiemodel onderscheidt toelichten en aan de hand van de antwoorden doorvragen.

4. Organisatie van botnetbestrijding

De volgende interviewvragen dienen om te beoordelen over welke competenties en bevoegdheden de organisatie beschikt die voor de bestrijdingsmethoden nodig zijn. Deze gegevens zijn nodig voor het beantwoorden van onderzoeksvraag [E.4] Een competentie wordt hier beschouwd als het vermogen waarover een organisatie beschikt, ofwel de informatie, kennis, vaardigheden en middelen die nodig zijn om botnetbestrijdingsmethoden effectief toe te passen. Een bevoegdheid is de autorisatie om een competentie te mogen aanwenden.

Per bestrijdingsmethode:

I.11. Over welke competenties (informatie, kennis, vaardigheden en middelen) beschikt uw organisatie om de bestrijdingsmethode te kunnen toepassen?

Per competentie:

I.11.1. Zit er enige wettelijke restrictie op de aanwending van de competentie? Zo ja, is uw organisatie wettelijk bevoegd de competentie aan te wenden?
I.11.2. In welke situaties, bijvoorbeeld bij wat voor soort botnet (naar oogmerk, commandostructuur of andere indeling) maakt u gebruik van de competentie?
I.11.3. Komen de competenties en bevoegdheden overeen met de die van het referentiemodel? Zo nee, waar zitten de verschillen?

De interviewer zal de competenties en bevoegdheden van het referentiemodel toelichten en aan de hand van de antwoorden doorvragen.

I.12. Voor welke aspecten van botnetbestrijding beschikt uw organisatie niet over de benodigde bevoegdheden of competenties?
I.13. Met welke organisaties wordt wegens een (gedeeltelijk) gebrek aan competenties of bevoegdheden samengewerkt?

Per externe organisatie waarmee wordt samengewerkt:

I.13.1. Welke bevoegdheden en competenties die de externe organisatie heeft of zou moeten hebben, betreft het?
I.13.2. Indien het gaat om een gebrek aan bevoegdheden: worden eigen competenties aangewend onder auspiciën van een externe bevoegde organisatie, of maakt de externe organisatie bij de uitoefening van haar bevoegdheden gebruik van eigen competenties?
I.13.3. Beoordeelt u de samenwerking met de externe organisatie als effectief? Zo nee, waarom niet?
I.13.4. Heeft de externe organisatie bepaalde bevoegdheden en/of competenties niet, die deze organisatie wel zou moeten hebben om effectief te zijn? Zo ja, welke?

5. Effectiviteit van botnetbestrijding in Nederland

De volgende vragen lopen vooruit op de analyse van de onderzoeksgegevens die met bovenstaande vragen zijn verkregen en zullen worden geanalyseerd aan de hand van het referentiemodel.

I.14. Zijn de verschillende organisaties die zich in Nederland met botnetbestrijding bezig houden in staat dat effectief te doen?

Zo ja:

I.14.1. Waaruit blijkt dat naar uw mening?

Zo nee:

I.14.2. Zijn er bestrijdingsmethoden die, door gebrek aan competenties, bevoegdheden of om andere redenen, niet in praktijk kunnen worden gebracht? Zo ja, welke?

I.14.3. Zijn er soorten botnets die naar uw mening daarom niet (afdoende) kunnen worden bestreden?

I.15. Zijn er naast de competenties en bevoegdheden nog andere aspecten die belangrijk zijn voor botnetbestrijding, maar die in het interview onderbelicht zijn gebleven?

6. Afsluiting van het interview

6.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, gezichtspunten of aanbevelingen voor het onderzoek te geven.

I.16. Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?

6.2. Afsluitende opmerkingen

De geïnterviewden worden bedankt voor hun medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek.

Bijlage F. Interviewverslagen

Appendix 1. NCTV / NCSC

1. Inleiding

Dit is het verslag van het onderzoeksinterview afgenomen met het Nationaal Cyber Security Centrum (NCSC) op 10 juni 2013 te Den Haag in vervolg op een eerder gesprek op 23 mei 2013 bij het Beleidscluster Cyber van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Het interview maakt deel uit van een afstudeeronderzoek aan de Faculteit Informatica van de Open Universiteit. Het onderzoek richt zich op de botnetbestrijding in Nederland. Het doel van dit interview is om op systematische wijze te inventariseren over welke competenties en bevoegdheden het NCSC beschikt om verschillende soorten botnets te kunnen bestrijden.

2. Algemene vragen over de organisatie

2.1. Geïnterviewden

I.1.1. ***Wat is uw naam (incl. voorletters, evt. rang en titels)?***
I.1.2. ***Wat is uw functie / relatie tot botnetbestrijding?***
I.1.3. ***Tot welke organisatie behoort u?***

In een eerder stadium is gesproken met Michel van Leeuwen, hoofd van de beleidscluster van de Directie Cyber Security van de NCTV. Op 10 juni zijn geïnterviewd:

Dave Woutersen, security specialist bij de afdeling Monitoring & Respons van het NCSC en heeft als incidentbehandelaar al ruim 9 jaar ervaring met onder meer botnets.

Justus van de Sande, beleidsadviseur bij de afdeling Ontwikkeling & Programma's van het NCSC, en als zodanig betrokken bij het uitvoeringsbeleid, o.m. voor botnetbestrijding.

2.2. Organisatie

I.2. ***Wat is de volledige naam van de organisatie? Wordt dit afgekort of zijn er andere aanduidingen voor de organisatie?***
I.3. ***Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?***

Geïnterviewden behoren tot het NCSC, dat valt onder de Directie Cyber Security van de NCTV.

Het NCSC heeft ongeveer 80 medewerkers en kent drie afdeling: 1. Expertise & Advies, 2. Monitoring & Respons (de CERT-rol), en 3. Ontwikkeling & Programma's (uitvoeringsbeleid en publiek-private samenwerking).

I.4. ***Indien van toepassing: wat is de rechtsbasis waaraan de organisatie haar bestaan en taken ontleent?***

Het NCSC ontleent haar bestaan aan de organisatieregeling van het Ministerie van Justitie; er bestaan geen wettelijke taken of bevoegdheden.

De missie van het NCSC luidt: "Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief."

Het NCSC richt zich primair op de veiligheid van computersystemen en – netwerken van de overheid, en de vitale infrastructuur (zoals energiesector, telecommunicatiebedrijven en banken). Daarnaast bedient het

NCSC de rest van de maatschappij met kennis en adviezen via zogenoemde schakelorganisaties, die zorgen voor de weerbaarheid van consumenten en organisaties in de niet-vitale infrastructuur.

I.5. ***Zijn er relevante openbare publicaties, zoals rapporten en jaarverslagen, van en over uw organisatie beschikbaar waarin cyber security in het algemeen of botnetbestrijding in het bijzonder aan de orde komen?***

Er is een algemeen jaarverslag van het NCTV. Specifiek op het gebied van cyber brengt het NCTV jaarlijks een Cybersecuritybeeld uit.

2.3. Andere organisaties

I.6. ***Welke andere organisaties die zich bezighouden met botnetbestrijding in Nederland zijn u bekend?***

Per bekende organisatie:

- I.6.1. ***Wat is de naam van die organisatie?***
- I.6.2. ***Wat voor soort organisatie betreft het?***
- I.6.3. ***Publieke organisatie?***
- I.6.4. ***Private organisatie: internetaanbieder / beveiligingsbedrijf / vitaal bedrijf / anders?***
- I.6.5. ***Werkt u ook samen met die organisatie? Ad hoc of structureel?***

Met internetaanbieders en SIDN wordt samengewerkt. Die samenwerking bestaat hoofdzakelijk uit het delen van informatie over geïnfecteerde IP-adressen; dit gebeurt structureel, is niet vastgelegd in wet- en regelgeving of overeenkomsten, maar volgt uit de taak van het NCSC. Daarnaast bestaat er de Notice-and-Take-Down procedure, waarbij een melding (notice) wordt gedaan van ongewenst of strafbare feiten door een klant van een internetaanbieder/hostingprovider, met het verzoek hier actie op te ondernemen. Dit is echter niet verplicht.

Met het Team High Tech Crime van de Politie en Inlichtingendiensten wordt structureel samengewerkt met liaisonfunctionarissen, zowel beleidsmatig als voor maken van het cybersecuritybeeld, en om bij de bestrijding van dreigingen gezamenlijk prioriteiten te stellen.

Strafrechtketen: OM, Politie en NFI wordt structureel samengewerkt met liaisonfunctionarissen.

Met het Ministerie van Economische Zaken wordt op thema's samengewerkt. Dit ministerie stimuleert verschillende activiteiten op het gebeid van botnetbestrijding. Voorbeelden hiervan zijn de *Abuse Information Exchange* voor informatie-uitwisseling over botnets tussen Internetaanbieders, en de Werkgroep Botnets van het Elektronisch Consumenten Platform (ECP).

Met de Autoriteit Consument en Markt (ACM) wordt samengewerkt. De ACM is de toezichthouder voor telecommunicatie en kan bestuursrechtelijk optreden tegen bijvoorbeeld SPAM

Binnen Defensie wordt vooral samengewerkt met DefCERT, die een uitwijkfaciliteit voor het NCSC biedt. De samenwerking met de krijgsmacht als zodanig is nog in ontwikkeling, omdat zij nog hun eigen rol in het eigen domein aan het vormgeven zijn.

Het NCSC werkt ook samen met private computerbeveiligingsbedrijven, zoals Fox-IT, ITsec, Madison Gurkha, KPMG, Deloitte, anti-virusbedrijven als Norton, Kaspersky, etc.. Dit gebeurt meestal ad hoc / op projectbasis.

Naast directe (bilaterale) samenwerking met genoemde partijen, zijn er diverse formele en informele overlegfora waarin het NCSC participeert.

I.7. ***Met welke internationale organisaties werkt u samen?***

Het NCSC treedt op als nationaal aanspreekpunt van de overheid voor internationale publieke en private organisaties.

Met internationale cyber security samenwerkingsverbanden waarin CERTs zijn verbonden, zoals de European Government CERTs (EGC) en het Forum of Incident Response and Security Teams (FIRST) wordt samengewerkt.

Met Microsoft als grootste internationaal computerbedrijf wordt structureel samengewerkt met een liaisonfunctionaris. Maar zo nodig wordt ook met andere internationale computer(beveiligings)bedrijven informatie uitgewisseld.

3. Botnetclassificatie en -bestrijdingsmethoden

3.1. Botnetclassificatie

I.8. ***Gebruikt uw organisatie een indeling, classificatie of taxonomie om verschillende soorten botnets te onderscheiden?***

I.9. ***Zo ja, is dit een indeling, classificatie of taxonomie gebaseerd op:***

a. ***de intentie van het botnet?***

b. ***de commandostructuur van het botnet?***

Indien één van bovenstaande indelingen wordt gehanteerd, per indeling:

I.9.1. ***Komt de gehanteerde indeling overeen met de taxonomie van het referentiemodel? Waar zitten de verschillen?***

Indien een andere indeling, classificatie of taxonomie wordt gehanteerd:

I.9.2. ***Wat voor botnetindeling, -classificatie of -taxonomie hanteert uw organisatie?***

I.9.3. ***Wat zijn de redenen om voor een dergelijke indeling te kiezen?***

Vanuit de rol van Nationale CERT wordt in beginsel geen onderscheid gemaakt in soorten botnets, omdat zij incidentgedreven werken en niet bij voorbaat een botnet classificeren. Wel is het van belang of de infrastructuur van het botnet zich (deels) in Nederland bevindt, of dat het doel van de aanvallen van het botnet zich in Nederland bevindt; dit is namelijk bepalend voor de rolinvulling door het NCSC.

Vanuit het oogpunt van de afdeling Expertise & Advies is een soortgelijke indeling als in het referentiemodel (naar structuur en intentie) wel van belang omdat dit een beeld geeft van het fenomeen botnet en waar beleidsmatig het aandachtspunt zal moeten liggen.

3.2. Botnetbestrijdingsmethoden

I.10. ***Op welke wijze of met welke methoden bestrijdt uw organisatie botnets? Met andere woorden: hoe gaat uw organisatie te werk?***

I.10.1. ***Bij wat voor soort botnets (conform de besproken classificatie) past u deze bestrijdingsmethode toe?***

I.10.2. ***Richt deze methode zich (primair) op individuele bots, de structuur van het botnet of tegen de botmaster?***

I.10.3. ***Komen de gehanteerde bestrijdingsmethoden overeen met de methoden in het referentiemodel? Waar zitten de verschillen?***

Verwijderen van bots uit een botnet door signaleringsfunctie (aangeven van besmettingen) naar overheidsorganisaties, vitale bedrijven en internetaanbieders.

Uitschakelen van commandoservers middels een Notice & Take-Down procedure.

Verstoring van het botnet door manipulatie van de communicatie, bijvoorbeeld sinkholing i.s.m. internetaanbieders.

4. Organisatie van botnetbestrijding

I.11. ***Over welke competenties (informatie, kennis, vaardigheden en middelen) beschikt uw organisatie om de bestrijdingsmethode toe te kunnen passen?***

Per competentie:

I.11.1. ***Zit er enige wettelijke restrictie op de aanwending van de competentie? Zo ja, is uw organisatie wettelijk bevoegd de competentie aan te wenden?***

I.11.2. ***In welke situaties, bijvoorbeeld bij wat voor soort botnet (naar oogmerk, commandostructuur of andere indeling) maakt u gebruik van de competentie?***

Competenties voor de opsporing van botnets:

(*op verzoek van de NCTV is dit antwoord weggelaten uit het eindverslag*)

Competenties voor de bestrijding van botnets:

Het verwijderen van botagents van computers (op een eigen netwerk) (C6) is geen taak van het NCSC; dat is binnen de overheid een taak van de beheersorganisaties van de verschillende computernetwerken, en daarbuiten van de private partijen zelf.

Het overnemen van een commandoserver (C7) of verstoring van het botnet met gemanipuleerde bots (C8) doet het NCSC niet, want dat is bij wet verboden.

Het verstoren of blokkeren van het botnet door manipulatie van de communicatie (C9) kan plaatsvinden in overleg met de ISP, door bijvoorbeeld de communicatie tussen commandoserver en bots af te vangen of te verhinderen (sinkholing).

Het overnemen van het botnet door manipulatie van de communicatie (C10) gebeurt niet door het NCSC.

Het regulier opsporen van de botmaster (C12), in beslag nemen van een commandoserver / computermateriaal (C13), veiligstellen van bewijsmateriaal (C14), en het arresteren en vervolgen van de botmaster(s) (C15) is een taak van de politie. Wel kan het NCSC niet-forensisch bewijsmateriaal leveren.

Een andere wijze om een commandoserver van een botnet uit te schakelen is via een Notice-and-Take-Down procedure, waarbij de activiteiten van de server aan de hostingprovider kenbaar worden gemaakt en die daarop actie kan ondernemen als de activiteiten de gebruiksvoorwaarden schenden of als daarmee de wet wordt overtreden.

Het NCSC houdt zich niet bezig met het op bijzondere wijze opsporen van de botmaster in het buitenland (C16) of het fysiek uitschakelen van botmaster(s) en/of infrastructuur (C17).

Overige competenties:

Samenwerking en coördinatie voor botnetbestrijding (C18) is de belangrijkste taak voor NCSC, zowel strategisch / beleidsmatig, maar ook operationeel (bestrijden specifiek botnet) door de juiste partijen tijdig te informeren.

(Wetenschappelijk) onderzoek (ten behoeve van alle andere competenties) op het gebied van botnetbestrijding (C19) doet het NCSC in beginsel niet zelf, maar er wordt wel samengewerkt met onderzoeksinstituten en universiteiten, zoals de TU Delft.

I.11.3. ***Komen de competenties en bevoegdheden overeen met de die van het referentiemodel? Zo nee, waar zitten de verschillen?***

Uit het gesprek blijkt dat de NTD-procedure niet expliciet in het referentiemodel is opgenomen, alleen ‘terughacken’ en het fysieke beslag op een server zijn genoemd.

I.12. ***Voor welke aspecten van botnetbestrijding beschikt uw organisatie niet over de benodigde bevoegdheden of competenties?***

I.13. ***Met welke organisaties wordt wegens een (gedeeltelijk) gebrek aan competenties of bevoegdheden samengewerkt?***

Per externe organisatie waarmee wordt samengewerkt:

I.13.1. ***Welke bevoegdheden en competenties die de externe organisatie heeft of zou moeten hebben, betreft het?***

I.13.2. ***Indien het gaat om een gebrek aan bevoegdheden: worden eigen competenties aangewend onder auspiciën van een externe bevoegde organisatie, of maakt de externe organisatie bij de uitoefening van haar bevoegdheden gebruik van eigen competenties?***

Politie en internetaanbieders (zie antwoorden op vraag 11).

I.13.3. ***Beoordeelt u de samenwerking met de externe organisatie als effectief? Zo nee, waarom niet?***

Ja, het is volgens geïnterviewden duidelijk wie welke taken en bevoegdheden heeft. Zo heeft iedere organisatie een duidelijke focus aansluitend bij de eigen taakstelling, en, waar nodig, wordt expertise gedeeld.

I.13.4. ***Heeft de externe organisatie bepaalde bevoegdheden en/of competenties niet, die die organisatie wel zou moeten hebben om effectief te zijn? Zo ja, welke?***

(*op verzoek van de NCTV is dit antwoord weggelaten uit het eindverslag*)

5. Effectiviteit van botnetbestrijding in Nederland

I.14. ***Zijn de verschillende organisaties die zich in Nederland met botnetbestrijding bezig houden in staat dat effectief te doen?***

Zo ja:

I.14.1. ***Waar blijkt dat naar uw mening uit?***

Eenmaal ontdekte botnets in Nederland zijn technisch gezien effectief te bestrijden. De samenwerking van betrokken partijen daarbij is goed te noemen, hoewel webhosters over het algemeen nog niet in dezelfde mate als internetaanbieders meewerken aan de bestrijding van botnets bij NTD-procedures.

Zo nee:

I.14.2. ***Zijn er bestrijdingsmethoden die, door gebrek aan competenties, bevoegdheden of om andere redenen, niet in praktijk kunnen worden gebracht? Zo ja, welke?***

De bestrijding van buitenlandse botnets blijft lastig, ook omdat de pakkans van botmasters dan betrekkelijk laag is. Maar dat is juist een reden om op botnetbestrijding te blijven inzetten, zodat Nederland een voortrekkersrol kan blijven spelen en de internationale samenwerking en het niveau van botnetbestrijding beter wordt.

Botnets, of symptomen ervan, worden niet altijd herkend door particulieren of politie, bijvoorbeeld bij aangifte van computercriminaliteit bij de lokale politie, en voor relatieve '*low-tech*' botnets is dus minder aandacht. Hierdoor zijn er botnets die onopgemerkt blijven.

I.14.3. ***Zijn er soorten botnets die naar uw mening daarom niet (afdoende) kunnen worden bestreden?***

Met name internationale botnets zijn moeilijk te bestrijden.

Hoewel de noodzaak op dit moment misschien niet dringend is, is meer onderzoek nodig naar de bestrijding van P2P-botnets. Het is waarschijnlijk dat, als botnetbestrijding effectiever gaat worden, dit type botnet meer aandacht en andere competenties voor de bestrijding zal gaan vragen.

I.15. ***Zijn er naast de competenties en bevoegdheden nog andere aspecten die belangrijk zijn voor botnetbestrijding, maar die in het interview onderbelicht zijn gebleven?***

Beveiliging tegen en bestrijding van botnets, en cyberdreiging in het algemeen, zal naar mening van geïnterviewden een '*way-of-living*' worden. Mensen en organisaties moeten zich bewust worden van een goede 'internet-hygiëne'.

6. Afsluiting van het interview

6.1. Slotvragen

I.16. ***Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?***

Nee.

Er wordt nog een korte rondleiding door het NCSC gegeven.

6.2. Afsluitende opmerkingen

De geïnterviewden worden bedankt voor hun medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek.

Appendix 2. Openbaar Ministerie

1. Inleiding

Dit is het verslag van het onderzoeksinterview afgenomen met het Openbaar Ministerie (OM) op 05 juni 2013 te Rotterdam. Het interview maakt deel uit van een afstudeeronderzoek aan de Faculteit Informatica van de Open Universiteit. Het onderzoek richt zich op de botnetbestrijding in Nederland. Het doel van dit interview is om op systematische wijze te inventariseren over welke competenties en bevoegdheden het OM beschikt om verschillende soorten botnets te kunnen bestrijden.

2. Algemene vragen over de organisatie

2.1. Geïnterviewden

I.1.1. ***Wat is uw naam (incl. voorletters, evt. rang en titels)?***
I.1.2. ***Wat is uw functie / relatie tot botnetbestrijding?***
I.1.3. ***Tot welke organisatie behoort u?***

Mr. L.J.A. (Lodewijk) van Zwieten, Landelijk Officier van Justitie voor Cybercrime met een tweeledige rol: 1. stuurt als Themaverantwoordelijk Officier het Team High Tech Crime van de politie aan; en 2. coördineert binnen het OM als landelijk officier voor cyber de aanpak van cybercrime door officieren van justitie.

2.2. Organisatie

I.2. ***Wat is de volledige naam van de organisatie? Wordt dit afgekort of zijn er andere aanduidingen voor de organisatie?***
I.3. ***Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?***

Geïnterviewde behoort tot de het Landelijk Parket van het Openbaar Ministerie (OM). Het Landelijk Parket bestrijdt (inter)nationaal georganiseerde misdaad en geeft daartoe leiding aan de opsporingsonderzoeken van de Nationale Recherche, die zich in het bijzonder richt op: de internationale handel in en smokkel van mensen, cocaïne, heroïne, vuurwapens en explosieven, de productie en export van synthetische drugs, witwassen van misdaadgeld, terrorisme en *high tech crime*. Het landelijk parket heeft een klein kennis- en expertisecentrum op het gebied van cyber.

I.4. ***Indien van toepassing: wat is de rechtsbasis waaraan de organisatie haar bestaan en taken ontleent?***

Het OM ontleent haar bestaan en taken aan het Wetboek van Strafvordering.

I.5. ***Zijn er relevante openbare publicaties, zoals rapporten en jaarverslagen, van en over uw organisatie beschikbaar waarin cyber security in het algemeen of botnetbestrijding in het bijzonder aan de orde komen?***

Er is een algemeen jaarverslag van het gehele OM waarin de cybercriminaliteit als onderdeel is opgenomen. (*Red.: In het "Jaarbericht 2012" staat een hoofdstuk over de proactieve en programmatische bestrijding cybercrime*) Over individuele zaken zijn er reguliere persberichten. Overige informatie is in principe alleen intern OM.

2.3. Andere organisaties

I.6. ***Welke andere organisaties die zich bezighouden met botnetbestrijding in Nederland zijn u bekend?***

Per bekende organisatie:

- I.6.1. ***Wat is de naam van die organisatie?***
- I.6.2. ***Wat voor soort organisatie betreft het?***
- I.6.3. ***Publieke organisatie?***
- I.6.4. ***Private organisatie: internetaanbieder / beveiligingsbedrijf / vitaal bedrijf / anders?***
- I.6.5. ***Werkt u ook samen met die organisatie? Ad hoc of structureel?***

Het OM werkt op cybergebied samen met de politie, in het bijzonder het Team High Tech Crime. Deze samenwerking is structureel in de wet verankerd omdat het OM de leiding heeft over een opsporingsonderzoek.

Het OM werkt samen met het Nationaal Cyber Security Centrum (NCSC). Dit is een structurele samenwerking gericht op informatie-uitwisseling en coördinatie middels liaisonfunctionarissen.

Met het Nederlands Forensisch Instituut (NFI) wordt samengewerkt, een publieke organisatie die ondersteuning en onafhankelijke expertise levert door analyse en duiding van bewijsmateriaal.

Het OM werkt ook samen met private computerbeveiligingsbedrijven, zoals Fox-IT, anti-virusbedrijven als Norton, Kasperski, etc. Dit gebeurt meestal ad hoc / op projectbasis wanneer in een bepaalde zaak behoefte is aan specifieke expertise voor de opsporing of het verkrijgen van bewijs.

Met de krijgsmacht en de inlichtingendiensten wordt zo nodig samengewerkt. Deze samenwerking kan als structureel worden geduid omdat die in de wet is verankerd, en overigens niet alleen op het gebied cyber van toepassing is. Op grond van de Wet op de Inlichtingen- en Veiligheidsdiensten bestaat de verplichting tot het delen van informatie, en de krijgsmacht levert indien nodig hulp en bijstand op basis van bestaande wet- en regelgeving. Van bijstand door de krijgsmacht specifiek op cybergebied is geen voorbeeld bekend.

Daarnaast maakt geïnterviewde melding van een aantal samenwerkingsinitiatieven: ECTF bij het THTC, en Abuse Information Exchange (IX) voor informatie-uitwisseling over botnets bij internetaanbieders.

I.7. ***Met welke internationale organisaties werkt u samen?***

Er wordt met opsporingsinstanties uit andere landen samengewerkt. Dit is ook structureel van aard en niet uitsluitend van toepassing op cybercrime. De prioriteit die andere landen aan botnetbestrijding geven, is niet altijd groot.

Het European Cybercrime Centre (EC3) moet zorgen voor centrale informatiedeling, waardoor deelnemende Europese landen niet direct zijn aangewezen op rechtshulpverzoeken.

Daarnaast werkt het OM zo nodig ook samen met (internationale) computerbedrijven, zoals Microsoft en Google. Het gaat dan meestal om ad hoc informatie-uitwisseling.

3. Botnetclassificatie en -bestrijdingsmethoden

3.1. Botnetclassificatie

I.8. ***Gebruikt uw organisatie een indeling, classificatie of taxonomie om verschillende soorten botnets te onderscheiden?***

I.9. ***Zo ja, is dit een indeling, classificatie of taxonomie gebaseerd op:***

a. ***de intentie van het botnet?***

b. ***de commandostructuur van het botnet?***

Indien één van bovenstaande indelingen wordt gehanteerd, per indeling:

I.9.1. ***Komt de gehanteerde indeling overeen met de taxonomie van het referentiemodel? Waar zitten de verschillen?***

Indien een andere indeling, classificatie of taxonomie wordt gehanteerd:

I.9.2. ***Wat voor botnetindeling, -classificatie of -taxonomie hanteert uw organisatie?***

I.9.3. ***Wat zijn de redenen om voor een dergelijke indeling te kiezen?***

Het strafbare feit is altijd leidend voor het OM, dus het OM zal in eerste aanleg altijd op basis daarvan classificeren.

In tweede aanleg is enerzijds het effect dat het feit teweeg brengt en anderzijds wat opsporingstechnisch haalbaar is, van belang. In die zin zijn respectievelijk de intentie en de structuur van het botnet zoals in het referentiemodel indirect wel van invloed.

Het OM ziet ook de scheiding tussen strafrecht en volkenrecht bij gebruik van botnets voor 'cyberwarfare' zoals gedefinieerd in het literatuuronderzoek.

3.2. Botnetbestrijdingsmethoden

I.10. ***Op welke wijze of met welke methoden bestrijdt uw organisatie botnets? Met andere woorden: hoe gaat uw organisatie te werk?***

I.10.1. ***Bij wat voor soort botnets (conform de besproken classificatie) past u deze bestrijdingsmethode toe?***

I.10.2. ***Richt deze methode zich (primair) op individuele bots, de structuur van het botnet of tegen de botmaster?***

I.10.3. ***Komen de gehanteerde bestrijdingsmethoden overeen met de methoden in het referentiemodel? Waar zitten de verschillen?***

Het OM ziet de bestrijding van botnets in drie stappen: 1. *intelligence*, 2. *interventions* en 3. *investigations*, waarbij men zich op drie aspecten richt: A. de infrastructuur van het botnet, B. de botmaster en C. de slachtoffers. De lijnen komen in beginsel overeen met de drie hoofdvormen om botnets te bestrijden in het referentiemodel, hoewel niet alle specifieke methoden worden toegepast.

A. Het aangrijpen van de botnetstructuur gebeurt beperkt op basis van de politiewet (handhaving orde en hulpverleningstaken van de politie): overname of uitschakeling van commandoservers komt voor, maar verstoring met gemanipuleerde bots niet; overname/verstoring van de communicatie gebeurt beperkt, en vereist medewerking van de internetaanbieder of hostingprovider.
B. Opsporen en arresteren van de botmaster voor strafrechtelijke vervolging is de kerntaak van het OM.
C. Het aangrijpen van de bots gebeurt niet direct door het OM, maar door notificatie aan slachtoffers.

4. Organisatie van botnetbestrijding

I.11. ***Over welke competenties (informatie, kennis, vaardigheden en middelen) beschikt uw organisatie om de bestrijdingsmethode toe te kunnen passen?***

Per competentie:

I.11.1. ***Zit er enige wettelijke restrictie op de aanwending van de competentie? Zo ja, is uw organisatie wettelijk bevoegd de competentie aan te wenden?***

I.11.2. ***In welke situaties, bijvoorbeeld bij wat voor soort botnet (naar oogmerk, commandostructuur of andere indeling) maakt u gebruik van de competentie?***

I.11.3. ***Komen de competenties en bevoegdheden overeen met de die van het referentiemodel? Zo nee, waar zitten de verschillen?***

Het regulier opsporen van de botmaster (C12) door opsporingsinstanties in Nederland of met medewerking van autoriteiten in het buitenland (m.b.v. rechtshulpverzoeken), het in beslag nemen van een commandoserver / computermateriaal, het veiligstellen van bewijsmateriaal (zowel fysiek als digitaal) (C14) en het arresteren en vervolgen van de botmaster(s) (C15), zijn de kerntaken van het OM, dat samen met de politie daarvoor over de juiste competenties en bevoegdheden beschikt.

Maar het OM heeft geen centraal sturende rol in de coördinatie voor botnetbestrijding (C18). De vraag is ook of botnetbestrijding centraal moet worden aangestuurd; volgens geïnterviewde is het beter om aan de hand van een leidraad en goede afbakening van verantwoordelijkheden alle betrokkenen hun eigen rol hierin te laten uitvoeren.

Het OM beschikt over een eigen kennis & expertisecentrum voor onderzoek (ten behoeve van alle andere competenties) op het gebied van botnetbestrijding (C19); deze expertise is wel primair juridisch / strafvorderlijk gericht.

Geïnterviewde geeft geen competenties aan die niet onder één van de voorgelegde competenties uit het model vallen.

I.12. ***Voor welke aspecten van botnetbestrijding beschikt uw organisatie niet over de benodigde bevoegdheden of competenties?***

Het OM houdt zich niet bezig met het zoeken naar botnets. Zowel het detecteren van bots en botnets op internet met een honeynet (C1) en het detecteren van bots en botnets op een specifiek netwerk met passieve methoden (C2) zijn geen taken van het OM maar verantwoordelijkheden van de eigenaren van de computersystemen. Het traceren van adressen / computers op internet (C11) is een taak van de politie, maar in principe kan iedereen die uitvoeren met behulp van beschikbare (openbare) gegevens.

Het verwijderen van botagents van computers (op een eigen netwerk) (C6) is geen taak van het OM. Deze competentie is dus niet nodig. Wel ziet het OM een rol (voor de politie) om slachtoffers van botnets te waarschuwen.

Het OM is niet bevoegd tot het opsporen van de botmaster in het buitenland (C16). Opsporing en vervolging in het buitenland vindt plaats via rechtshulpverzoeken aan buitenlandse opsporingsautoriteiten via reguliere opsporingsmethoden (C12).

I.13. ***Met welke organisaties wordt wegens een (gedeeltelijk) gebrek aan competenties of bevoegdheden samengewerkt?***

Per externe organisatie waarmee wordt samengewerkt:

- I.13.1. ***Welke bevoegdheden en competenties die de externe organisatie heeft of zou moeten hebben, betreft het?***
- I.13.2. ***Indien het gaat om een gebrek aan bevoegdheden: worden eigen competenties aangewend onder auspiciën van een externe bevoegde organisatie, of maakt de externe organisatie bij de uitoefening van haar bevoegdheden gebruik van eigen competenties?***
- I.13.3. ***Beoordeelt u de samenwerking met de externe organisatie als effectief? Zo nee, waarom niet?***
- I.13.4. ***Heeft de externe organisatie bepaalde bevoegdheden en/of competenties niet, die die organisatie wel zou moeten hebben om effectief te zijn? Zo ja, welke?***

Het onderzoeken van specifieke malware (software van botagents) op gedrag en eigenschappen (C3) is een taak van computerbeveiligingsbedrijven en in specifieke gevallen (voor bewijsvoering) van het NFI.

Het onderzoeken van de eigenschappen en het gedrag van specifieke botnets (C4) (met behulp van een honeynet / door infiltratie met botagents / door afvangen van botnetdataverkeer / door manipulatie van het commandokanaal / door overname van een commandoserver) doet het OM niet zelf, maar wordt namens het OM door de politie gedaan die hiervoor over de benodigde competentie beschikt. Van belang is de scheiding tussen actieve inmenging in botnet en passieve monitoring, vanwege privacy, voorkoming van schade aan computersystemen van anderen etc. Proportionaliteit is hierbij het uitgangspunt: de gebruikte opsporingsmethoden moeten in verhouding staan tot het strafbare feit. Daarbij komt dat wanneer een botnet de belangen van meer dan één partij schaadt, ingrijpender opsporingsmethoden kunnen worden gebruikt. Medewerking van derden, zoals een aangevallen vitaal bedrijf, computerbeveiligingsbedrijven, internetaanbieder, etc. wordt dan ook belangrijker.

Voor het achterhalen van encryptiesleutels en ontcijferen van informatie (C5) wordt gebruik gemaakt van politie of zo nodig van private computerbeveiligingsbedrijven.

Het overnemen (en uitschakelen) van een commandoserver (C7) om een botnet uit te schakelen kan worden gedaan door de politie. Dit wordt in aanvulling op het onderzoek naar het botnet (C4) primair gezien als een ordehandhavingsmaatregel die op basis van de politiewet wordt uitgevoerd, maar wordt door het OM gedekt. De politie zal niet het botnet overnemen en bijvoorbeeld geen opdrachten geven aan botagent*s* om zichzelf te wissen, omdat actieve opdrachten geven aan computers van slachtoffers als te risicovol wordt gezien; hoogstens worden slachtoffers van het botnet gewaarschuwd.

Het OM ziet voor toepassing van deze methode uitsluitend een taak voor het OM / politie, omdat het overnemen van een computer van iemand anders als een ingrijpende methode wordt gezien, en alleen een publieke organisatie hier op de juiste wijze verantwoording over kan afleggen. Ook hier geldt dat er telkens een goede belangenafweging moet worden gemaakt tussen enerzijds het wegnemen van de dreiging / de verstoring door het botnet, en anderzijds de strafrechtelijke opsporing.

In aanvulling hierop kan door manipulatie van de communicatie het botnet worden verstoord (zgn. '*sinkhole*') (C9); dit gebeurt i.s.m. de politie en zo nodig met internetaanbieders. Proportionaliteit is ook hierbij het uitgangspunt: de gebruikte handhavingsmethode moeten in verhouding staan tot de door het botnet veroorzaakte verstoring. Geavanceerdere actieve methoden, zoals verstoring met eigen ingebrachte bots (C8) of overname van het botnet door manipulatie van de communicatie (C10), worden daarom niet toegepast.

Het veiligstellen van bewijsmateriaal (zowel fysiek als digitaal) (C14) gebeurt in samenwerking met het NFI als onafhankelijke onderzoeksinstantie aan de hand van forensisch technische normen.

5. Effectiviteit van botnetbestrijding in Nederland

I.14. ***Zijn de verschillende organisaties die zich in Nederland met botnetbestrijding bezig houden in staat dat effectief te doen?***

Zo ja:

I.14.1. ***Waar blijkt dat naar uw mening uit?***

Zo nee:

I.14.2. ***Zijn er bestrijdingsmethoden die, door gebrek aan competenties, bevoegdheden of om andere redenen, niet in praktijk kunnen worden gebracht? Zo ja, welke?***

I.14.3. ***Zijn er soorten botnets die naar uw mening daarom niet (afdoende) kunnen worden bestreden?***

Naar mening van geïnterviewde is Nederland nog niet effectief (genoeg) bij de bestrijding van botnets. Binnen de openbare orde, en dus in het cyberdomein, hebben publieke en private partijen ondanks verschillende verantwoordelijkheden wel een gezamenlijk belang. Het OM richt zich daarbinnen primair op de strafrechtelijke handhaving, maar de rechtsorde is slechts een deel van de openbare orde als geheel.

Ondanks het gezamenlijk belang, ontbreekt een gezamenlijke missie op het gebied van botnetbestrijding. Daardoor is er nog weinig samenhang in activiteiten die de verschillende organisaties ontplooien. Dit is op verschillende manieren merkbaar: zo moeten bijvoorbeeld wederzijdse inzichten van betrokken partijen beter worden gedeeld. De competenties om botnets te bestrijden, zijn over het algemeen aanwezig bij de gezamenlijk betrokken organisaties, maar de gezamenlijke focus en samenhang moeten nog verder worden ontwikkeld. De overheid zou hierin geen centrale sturende, maar wel een aanjagende rol moeten spelen.

Op sublandelijk niveau bij het OM en de politie, moeten de competenties op het gebied van computercriminaliteit nog verder groeien. Het Landelijk Parket en de Nationale Recherche houden zich namelijk vooral met de zware landelijk georganiseerde misdaad bezig. Maar het herkennen van en handelen op kleinere, plaatselijke misdrijven waarbij computers en botnets mogelijk een rol spelen, is ook belangrijk en moet nog verder worden ontwikkeld.

I.15. ***Zijn er naast de competenties en bevoegdheden nog andere aspecten die belangrijk zijn voor botnetbestrijding, maar die in het interview onderbelicht zijn gebleven?***

Nee.

6. Afsluiting van het interview

6.1. Slotvragen

I.16. ***Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?***

De geïnterviewde heeft geen aanvullende opmerkingen.

6.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men, wordt indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek.

Appendix 3. Politie

1. Inleiding

Dit is het verslag van het onderzoeksinterview afgenomen met het Team High Tech Crime (THTC) van de politie op 23 april 2013 te Driebergen. Het interview maakt deel uit van een afstudeeronderzoek aan de Faculteit Informatica van de Open Universiteit. Het onderzoek richt zich op de botnetbestrijding in Nederland. Het doel van dit interview is om op systematische wijze te inventariseren over welke competenties en bevoegdheden de politie beschikt om verschillende soorten botnets te kunnen bestrijden.

2. Algemene vragen over de organisatie

2.1. Geïnterviewden

I.1.1. ***Wat is uw naam (incl. voorletters, evt. rang en titels)?***

I.1.2. ***Wat is uw functie / relatie tot botnetbestrijding?***

Dhr. Ton Maas, digitaal coördinator, belast met de aansturing van onderzoeken, waaronder contacten leggen met betrokken partijen voor samenwerking.

Dhr. Frank Bernaards, beleidsadviseur met juridische achtergrond en belast met de afstemming van de taken van het THTC, waaronder botnetbestrijding, met hoger beleid en met (internationale) partners.

Dhr. Peter Wagenaar en Dhr. Daan de Graaf, beiden Digitaal Rechercheur en als zodanig belast met het opsporen van verdachten (botmasters/herders), met technisch sporenonderzoek en met uitschakeling van botnets.

I.1.3. ***Tot welke organisatie behoort u?***

Alle geïnterviewden behoren binnen de Landelijke Recherche van de Nationale Politie tot het Team High Tech Crime (THTC).

2.2. Organisatie

I.2. ***Wat is de volledige naam van de organisatie? Wordt dit afgekort of zijn er andere aanduidingen voor de organisatie?***

Nationale Politie / Landelijke eenheid / Landelijke Recherche / Team High Tech Crime (THTC). In het Engels: National High Tech Crime Unit.

I.3. ***Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?***

Het THTC groeit van 30 personen in 2007 naar ongeveer 120 personen in 2014, zodat er tussen de 15-20 grote zaken per jaar kunnen worden gedaan. Het THTC zal dan bestaan uit drie operationele teams (bestaand uit ieder twee secties) die elk over alle expertise beschikken om zelfstandig een zaak te kunnen onderzoeken. Een vierde team zorgt voor interne ondersteuning, voorbereiding en beleid. Bij het THTC is tevens de Electronic Crime Task Force (ECTF) ingebed, een multidisciplinair team dat met de banken samenwerkt.

I.4. ***Indien van toepassing: wat is de rechtsbasis waaraan de organisatie haar bestaan en taken ontleent?***

Het THTC ontleent haar bestaan en taken primair aan de Politiewet (art.3) en het Wetboek van Strafvordering (art.141 en 142).

I.5. ***Zijn er relevante openbare publicaties, zoals rapporten en jaarverslagen, van en over uw organisatie beschikbaar waarin cyber security in het algemeen of botnetbestrijding in het bijzonder aan de orde komen?***

Het hogere beleid wordt voor het THTC vertaald naar een visie- en strategiedocument. Samen met een Criminaliteitsbeeldanalyse wordt een Tactisch Programma opgesteld. [*De Criminaliteitsbeeldanalyse is na afloop van het interview ter beschikking gesteld.*]

2.3. Andere organisaties

I.6. ***Welke andere organisaties die zich bezighouden met botnetbestrijding in Nederland zijn u bekend?***

Per bekende organisatie:

- I.6.1. ***Wat is de naam van die organisatie?***
- I.6.2. ***Wat voor soort organisatie betreft het?***
- I.6.3. ***Publieke organisatie?***
- I.6.4. ***Private organisatie: internetaanbieder / beveiligingsbedrijf / vitaal bedrijf / anders?***
- I.6.5. ***Werkt u ook samen met die organisatie? Ad hoc of structureel?***

Het THTC werkt tevens samen met het Nationaal Cyber Security Centrum (NCSC). Dit is een structurele samenwerking, met name bij grote cyberincidenten. De samenwerking geschiedt vanuit ieders bevoegdheid: daar waar het NCSC zich richt op coördinatie en beperking van verstoring en schade door een botnet, richt het THTC zich hoofdzakelijk op strafbare feiten en het opsporen van de botmaster,

Het THTC werkt als onderdeel van de politie samen met het Landelijk Parket van het Openbaar Ministerie (OM). Deze samenwerking is structureel in de wet verankerd omdat het OM de leiding heeft over een opsporingsonderzoek.

Met het Nederlands Forensisch Instituut (NFI) wordt samengewerkt, een publieke organisatie die door tussenkomst van het OM ondersteuning en (onafhankelijk) expertise levert.

Het THTC werkt samen met aanbieders van internet- en computerdiensten (Internetproviders en Hostingproviders). Dit zijn private partijen met meestal eigen CERTs die waardevolle informatie kunnen verstrekken aan de politie wanneer hun diensten worden gebruikt door botnets. De samenwerking is meestal ad hoc, en soms structureler op projectbasis; in sommige gevallen is er geen sprake van samenwerking maar moet de politie haar bevoegdheid gebruiken om medewerking te verkrijgen.

Het THTC werkt ook samen met private computerbeveiligingsbedrijven. Dit gebeurt meestal ad hoc, maar er wordt aangestuurd op meer structurele samenwerking, met name op het gebied van kennis en expertise.

Met universiteiten wordt samengewerkt op kennis- en onderzoeksgebied, en soms voor ondersteuning.

I.7. ***Met welke internationale organisaties werkt u samen?***

Er wordt met opsporingsinstanties uit andere landen samengewerkt. Daarbij wordt gezocht naar een balans tussen formele en informele samenwerking, want formele rechtshulpverzoeken hebben veel overhead.

Het European Cybercrime Centre (EC3) moet zorgen voor centrale informatiedeling, waardoor deelnemende Europese landen niet direct zijn aangewezen op rechtshulpverzoeken. EC3 moet nog in die rol groeien; momenteel wordt vooral nog algemene informatie gedeeld, maar met het groeien van het onderling vertrouwen kan dat ook specifiekere informatie worden.

Daarnaast werkt THTC ook samen met (internationale) computerbedrijven, zoals Microsoft en Google. Het gaat dan meestal om ad hoc informatie-uitwisseling.

3. Botnetclassificatie en -bestrijdingsmethoden

3.1. Botnetclassificatie

I.8. ***Gebruikt uw organisatie een indeling, classificatie of taxonomie om verschillende soorten botnets te onderscheiden?***

I.9. ***Zo ja, is dit een indeling, classificatie of taxonomie gebaseerd op:***

a. ***de intentie van het botnet?***

b. ***de commandostructuur van het botnet?***

Indien één van bovenstaande indelingen wordt gehanteerd, per indeling:

I.9.1. ***Komt de gehanteerde indeling overeen met de taxonomie van het referentiemodel? Waar zitten de verschillen?***

Indien een andere indeling, classificatie of taxonomie wordt gehanteerd:

I.9.2. ***Wat voor botnetindeling, -classificatie of -taxonomie hanteert uw organisatie?***

I.9.3. ***Wat zijn de redenen om voor een dergelijke indeling te kiezen?***

Het THTC hanteert niet zozeer een indeling naar intentie van het botnet of de commandostructuur, zoals in het referentiemodel. Omdat de opsporing begint met een strafbaar feit, wordt in de eerste plaats een indeling gemaakt naar soort aanval en de impact van de aanval.

Daarnaast is van belang of de botmaster zich in Nederland bevindt of het botnet vanuit Nederland wordt aangestuurd, omdat dat bepalend is of Nederland rechtsmacht heeft en het THTC dus bevoegd is tot opsporing.

Wel wordt beleidsmatig aangestuurd om het verschijnsel botnets meer als één fenomeen te benaderen, wat de intentie van het botnet wel belangrijker zou maken en om proactiever botnetbestrijding uit te voeren.

Een indeling naar commandostructuur wordt ook wel gemaakt, maar is pas in tweede aanleg impliciet van belang. Er is wel een relatie tussen commandostructuur en aanvalsvorm; zo komt een P2P-botnet met name voor bij spam, maar dat is geen aanvalsvorm die voor het THTC van belang is, terwijl de zwaardere criminaliteit juist vaker gebruik maakt van relatief eenvoudige centraal aangestuurde botnets die verhuurd worden gebruikt.

3.2. Botnetbestrijdingsmethoden

I.10. ***Op welke wijze of met welke methoden bestrijdt uw organisatie botnets? Met andere woorden: hoe gaat uw organisatie te werk?***

I.10.1. ***Bij wat voor soort botnets (conform de besproken classificatie) past u deze bestrijdingsmethode toe?***

I.10.2. ***Richt deze methode zich (primair) op individuele bots, de structuur van het botnet of tegen de botmaster?***

I.10.3. ***Komen de gehanteerde bestrijdingsmethoden overeen met de methoden in het referentiemodel? Waar zitten de verschillen?***

Het THTC richt zich primair op het arresteren en vervolgen van de botmaster. ‘Botmaster’ moet hier breed worden gezien: dit kan degene zijn die technisch de controle over het botnet heeft, maar ook de persoon of organisatie die het botnet huurt, etc. ‘*follow the money*’

Het overnemen en uitschakelen van commandoservers door het THTC is in beginsel mogelijk. Het wordt echter niet als effectief gezien. Een server bevat vaak weinig of geen dadersporen en meestal hebben botmasters back-upservers (in een ander land) die na uitschakeling kunnen worden ingezet.

Verstoring door manipulatie van communicatie (bijvoorbeeld met een ‘*sinkhole*’), kan enerzijds uit opsporingsoogpunt worden gedaan (het dwingt de botmaster tot reactie waardoor kans op fouten en achterlaten van sporen groter wordt), anderzijds zou het kunnen gebeuren ter bescherming van slachtoffers van het botnet of beperking van schade.

Voor de keuze van de bestrijdingsmethode is een classificatie van het botnet naar bijvoorbeeld intentie, commandostructuur of aanvalsvormen niet van belang. De toe te passen bestrijdingsmethode hangt van veel factoren af en is zeer contextafhankelijk.

4. Organisatie van botnetbestrijding

I.11. ***Over welke competenties (informatie, kennis, vaardigheden en middelen) beschikt uw organisatie om de bestrijdingsmethode toe te kunnen passen?***

De politie beschikt over de volgende competenties ten aanzien van botnetbestrijding:

C3. Het onderzoeken van specifieke malware (software van botagents) op gedrag en eigenschappen (wat overigens vaak aan private computerbeveiligingsbedrijven wordt overgelaten)

C4. Het onderzoeken van de eigenschappen en het gedrag van specifieke botnets (met behulp van een honeynet / door infiltratie met botagents / door afvangen van botnetdataverkeer / door manipulatie van het commandokanaal / door overname van een commandoserver).

C5. Het achterhalen van encryptiesleutels en ontcijferen van informatie.

C7. Het overnemen van een commandoserver.

C9. Het verstoren of blokkeren van het botnet door manipulatie van de communicatie, bijvoorbeeld met een zgn. '*sinkhole*' (waar doorgaans wel medewerking van private computerbedrijven / netwerkeigenaar / internetaanbieders voor nodig is).

C11. Het traceren van adressen / computers op internet.

C12. Het regulier opsporen van de botmaster (door opsporingsinstanties in Nederland; met medewerking van autoriteiten in het buitenland)

C13. Het in beslag nemen van een commandoserver / computermateriaal.

C14. Het veiligstellen van bewijsmateriaal (zowel fysiek als digitaal).

C15. Het arresteren en vervolgen van de botmaster(s).

C18. Samenwerking en coördinatie voor botnetbestrijding.

C19. (Wetenschappelijk) onderzoek (ten behoeve van alle andere competenties) op het gebied van botnetbestrijding.

Per competentie:

I.11.1. ***Zit er enige wettelijke restrictie op de aanwending van de competentie? Zo ja, is uw organisatie wettelijk bevoegd de competentie aan te wenden?***

I.11.2. ***In welke situaties, bijvoorbeeld bij wat voor soort botnet (naar oogmerk, commandostructuur of andere indeling) maakt u gebruik van de competentie?***

Voor wat betreft competentie C4 (het onderzoeken van de eigenschappen en het gedrag van specifieke botnets met behulp van een honeynet / door infiltratie met botagents / door afvangen van botnetdataverkeer/ door manipulatie van het commandokanaal / door overname van een commandoserver) is de aanwending van de competenties gelimiteerd. Dit is erg contextafhankelijk, maar uitgangspunt is dat er niet meer of zwaardere middelen worden gebruik dan noodzakelijk.

Het verwijderen van malware (competentie C6) is geen politietaak, maar de politie ziet het, op basis van Art.3 van de politiewet, wel als haar taak om slachtoffers van een botnet te waarschuwen over de aanwezigheid van malware.

Het overnemen van een commandoserver (competentie C7) en die als zodanig gebruiken om een botnet aan te sturen en de werking ervan te verhinderen, is beperkt mogelijk; zo moet de server in Nederland staan en moet de impact van het botnet naar oordeel van het OM ernstig genoeg zijn om dit middel te gebruiken. (Onderzoek van een in beslaggenomen server valt overigens onder competenties C13/C14).

Voor competentie C9 is medewerking van private partijennodig.

I.11.3. ***Komen de competenties en bevoegdheden overeen met de die van het referentiemodel? Zo nee, waar zitten de verschillen?***

Geïnterviewden geven geen competenties aan die niet onder één van de voorgelegde competenties uit het model vallen.

I.12. ***Voor welke aspecten van botnetbestrijding beschikt uw organisatie niet over de benodigde bevoegdheden of competenties?***

I.13. ***Met welke organisaties wordt wegens een (gedeeltelijk) gebrek aan competenties of bevoegdheden samengewerkt?***

Per externe organisatie waarmee wordt samengewerkt:

I.13.1. ***Welke bevoegdheden en competenties die de externe organisatie heeft of zou moeten hebben, betreft het?***

I.13.2. ***Indien het gaat om een gebrek aan bevoegdheden: worden eigen competenties aangewend onder auspiciën van een externe bevoegde organisatie, of maakt de externe organisatie bij de uitoefening van haar bevoegdheden gebruik van eigen competenties?***

Voor het volgende beschikt het THTC niet over de competenties en/of bevoegdheden:

Het detecteren van bots en botnets op internet met een honeynet (competentie C1); dit zou uitlokking zijn. Het THTC is voor informatievergaring over bestudeerde botnets afhankelijk van partijen die wel botnetonderzoek met behulp van honeynets doen, zoals computerbeveiligingsbedrijven.

Het detecteren van bots en botnets op een specifiek netwerk met passieve methoden (competentie C2); dit zou betekenen dat de politie op netwerken van derden mee zou mogen kijken. Het THTC is in dezen afhankelijk van de medewerking / aangifte van internetbedrijven, private bedrijven etc. die botnets of botnetaanvallen op hun eigen netwerken en systemen detecteren.

Het komt voor dat bij het beslag leggen op een server en/of veiligstellen van bewijsmateriaal (competenties C13/14) gebruik wordt gemaakt van de ondersteuning door private partijen die fysiek toegang hebben tot de server en die deze acties uitvoeren onder auspiciën van de politie.

I.13.3. ***Beoordeelt u de samenwerking met de externe organisatie als effectief? Zo nee, waarom niet?***

De politie alleen is niet in staat botnets te bestrijden en heeft daarbij andere partijen nodig, met name de kennis en expertise van computer(beveiligings)bedrijven en medewerking van internet- en hostingproviders.

De geïnterviewden ervaren die noodzakelijke samenwerking met genoemde partijen wel als effectief: alle benodigde competenties van anderen ten behoeve van de taakuitvoering van het THTC kunnen in de praktijk worden aangewend wanneer nodig.

I.13.4. ***Heeft de externe organisatie bepaalde bevoegdheden en/of competenties niet, die die organisatie wel zou moeten hebben om effectief te zijn? Zo ja, welke?***

Vanuit het perspectief van THTC zijn daarmee alle benodigde competenties afgedekt om de taak te kunnen uitvoeren.

5. Effectiviteit van botnetbestrijding in Nederland

I.14. ***Zijn de verschillende organisaties die zich in Nederland met botnetbestrijding bezig houden in staat dat effectief te doen?***

Voor een belangrijk deel JA:

Zo ja:

I.14.1. ***Waar blijkt dat naar uw mening uit?***

Het voorbeeld van het Bredolab-botnet dat succesvol is bestreden, wordt onder meer genoemd.

Maar deels is het antwoord ook NEE:

Zo nee:

I.14.2. ***Zijn er bestrijdingsmethoden die, door gebrek aan competenties, bevoegdheden of om andere redenen, niet in praktijk kunnen worden gebracht? Zo ja, welke?***

De verschillende organisaties zijn in principe in staat het effectief te doen, maar er wordt momenteel nog primair reactief ingegrepen. De politie heeft dat onderkend en wil zelf proactiever optreden. Dat is in beginsel mogelijk omdat een botnet in zichzelf al strafbaar is (inherent aan het fenomeen). Dus er zijn in die zin geen beperkingen voor de politie om proactief de bestrijding op te pakken. Er zijn wel enige juridische kaders voor fenomeen-onderzoek in georganiseerd verband, onder meer vanwege (willekeurige) vergaring van persoonsgegevens en bewaartermijnen daarvan.

De grootste beperking is dat de politie niet bevoegd is computers op afstand te betreden. Dat betekent dat bepaalde competenties niet volledig (zelfstandig) kunnen worden benut. Dit is met name het geval voor C4 (het onderzoeken van de eigenschappen en het gedrag van specifieke botnets), C7 (het overnemen van een commandoserver) en C9 (het verstoren of blokkeren van het botnet door manipulatie van de communicatie). , maar

Verregaande vormen van tracering op internet (bijvoorbeeld met watermarking) zijn hierdoor ook zeer beperkt mogelijk, maar in de praktijk is dat geen belemmering voor competentie C11 (traceren op internet) omdat binnen Nederland tracering met meer traditionele opsporingmethoden voldoende blijkt en de complexiteit van dergelijke methoden niet opweegt tegen de resultaten ervan.

Daarentegen blijft het opsporen van een botmaster in het buitenland iets wat beperkt vanuit Nederland is af te dwingen. Met veel landen kan door middel van een rechtshulpverzoek opsporing in een betreffend land plaatsvinden, maar dat is voor een groot aantal landen niet haalbaar.

I.14.3. ***Zijn er soorten botnets die naar uw mening daarom niet (afdoende) kunnen worden bestreden?***

De geïnterviewden zijn van mening dat ondanks enige bovenstaande beperkingen en een verbetering met een meer proactieve aanpak in de toekomst, er in principe geen verschijningsvormen van botnets zijn die niet bestreden kunnen worden.

I.15. ***Zijn er naast de competenties en bevoegdheden nog andere aspecten die belangrijk zijn voor botnetbestrijding, maar die in het interview onderbelicht zijn gebleven?***

Vitale bedrijven, internetaanbieders en hostingproviders zouden meer werk moeten maken en actiever moeten samenwerken om botnets effectiever te kunnen bestrijden. Het fenomeen is te groot en kent teveel gradaties om de politie alles te laten oplossen. Maar voor commerciële partijen wegen daarbij andere belangen mee, zoals kosten.

Op internationaal terrein speelt ook nog het *incentive* probleem: diverse landen ondervinden hinder van een botnet, maar omdat niemand onevenredig hard getroffen wordt, ontbreekt de incentive om het botnet aan te pakken.

6. Afsluiting van het interview

6.1. Slotvragen

I.16. ***Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?***

De geïnterviewden hebben geen aanvullende opmerkingen.

6.2. Afsluitende opmerkingen

De geïnterviewden worden bedankt voor hun medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek.

Appendix 4. DefCERT

1. Inleiding

Dit is het verslag van het onderzoeksinterview afgenomen met DefCERT op 22 april 2013 te Soesterberg. Het interview maakt deel uit van een afstudeeronderzoek aan de Faculteit Informatica van de Open Universiteit. Het onderzoek richt zich op de botnetbestrijding in Nederland. Het doel van dit interview is om op systematische wijze te inventariseren over welke competenties en bevoegdheden DefCERT beschikt om verschillende soorten botnets te kunnen bestrijden.

2. Algemene vragen over de organisatie

2.1. Geïnterviewden

I.1.1. ***Wat is uw naam (incl. voorletters, evt. rang en titels)?***
I.1.2. ***Tot welke organisatie behoort u?***
I.1.3. ***Wat is uw functie / relatie tot botnetbestrijding?***

Het interview is afgenomen met Dhr. L. (Leon) van der Eijk, werkend als Senior Analist / Malware expert voor DefCERT, het Computer Emergency Response Team van het Ministerie van Defensie.

2.2. Organisatie

I.2. ***Wat is de volledige naam van de organisatie? Wordt dit afgekort of zijn er andere aanduidingen voor de organisatie?***
I.3. ***Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?***

DefCERT is het 'Defensie *Computer Emergency Response Team*'. Het is een zelfstandig functionerend organisatie-element, maar is organisatorisch ondergebracht bij het Joint Informatievoorzieningscommando (JIVC) dat onderdeel uitmaakt van de Defensie Materieel Organisatie (DMO). Functioneel raakt DefCERT enerzijds de Beveiligingsautoriteit en anderzijds de CIS / ICT-beheersorganisaties binnen het ministerie van Defensie en de krijgsmacht.

DefCERT bestaat uit 15 personen. De organisatie bestaat uit een hoofd en twee afdelingen:

1. Advies & Ondersteuning, dat zich richt op advies voor CIS / ICT-beheers- en projectorganisaties binnen het Ministerie van Defensie en de krijgsmacht.
2. Incident Response, dat zich richt op analyse van beveiligingsincidenten van systemen in gebruik bij het Ministerie van Defensie en de krijgsmacht.

I.4. ***Indien van toepassing: wat is de rechtsbasis waaraan de organisatie haar bestaan en taken ontleent?***

Er is geen specifieke rechtsbasis. DefCERT is als onderdeel van het ministerie van Defensie een publieke organisatie, maar richt zich nagenoeg uitsluitend op bescherming van informatiesystemen en netwerken van Defensie zelf, inclusief de krijgsmacht.

I.5. ***Zijn er relevante openbare publicaties, zoals rapporten en jaarverslagen, van en over uw organisatie beschikbaar waarin cyber security in het algemeen of botnetbestrijding in het bijzonder aan de orde komen?***

DefCERT rapporteert alleen intern aan het ministerie van Defensie en geeft geen eigen openbare publicaties uit.

2.3. Andere organisaties

I.6. ***Welke andere organisaties die zich bezighouden met botnetbestrijding in Nederland zijn u bekend?***

Per bekende organisatie:

I.6.1. ***Wat is de naam van die organisatie?***
I.6.2. ***Wat voor soort organisatie betreft het?***
I.6.3. ***Publieke organisatie?***
I.6.4. ***Private organisatie: internetaanbieder / beveiligingsbedrijf / vitaal bedrijf / anders?***
I.6.5. ***Werkt u ook samen met die organisatie? Ad hoc of structureel?***

DefCERT werkt samen met de Nationale Cyber Security Centrum (NCSC), een publieke organisatie. De samenwerking is structureel. NCSC zorgt vanuit de Rijksoverheid voor een algemene dreigingsanalyse/waakdienst rijksoverheid (de Nationale CERT-taak). Daarnaast biedt DefCERT een uitwijkmogelijkheid voor de NCSC en stelt back-ups van NCSC-systemen veilig.

DefCERT werkt structureel met Fox-IT samen. Fox-IT is een privaat computerbeveiligingsbedrijf. Vanwege de schaarste aan personeel heeft DefCERT met Fox-IT een kennisuitwisselingsprogramma.

DefCERT werkt met de Militaire Inlichtingen en Veiligheidsdienst (MIVD) samen. Die samenwerking is structureel, maar in praktijk eenrichtingsverkeer: DefCERT fungeert als informatiebron voor de MIVD, maar DefCERT kan geen informatie van de MIVD gebruiken en krijgt die ook niet ter beschikking.

Naast formele samenwerkingsvormen vindt er veel informele samenwerking en kennisuitwisseling plaats, bijvoorbeeld via de Nederlandse chapter 'HoneyNed' binnen honeynet.org, een non-profit organisatie.

DefCERT werkt niet samen met opsporingsdiensten in Nederland, ook niet met de Koninklijke Marechaussee die opsporingstaak heeft wanneer een aanval zich tegen de krijgsmacht richt. DefCERT werkt ook niet samen met de krijgsmacht in de uitvoering van de primaire taak van de krijgsmacht.

I.7. ***Met welke internationale organisaties werkt u samen?***

DefCERT werkt samen met NATO Computer Incident Response Capability (CIRC). Dat vindt vooral op ad-hocbasis plaats ten behoeve van kennisuitwisseling en gezamenlijke oefeningen.

DefCERT is lid van het Forum of Incident Response & Security Teams (FIRST), een internationaal samenwerkingsverband tussen private en publieke CERTs.

3. Botnetclassificatie en -bestrijdingsmethoden

3.1. Botnetclassificatie

I.8. ***Gebruikt uw organisatie een indeling, classificatie of taxonomie om verschillende soorten botnets te onderscheiden?***
I.9. ***Zo ja, is dit een indeling, classificatie of taxonomie gebaseerd op:***
a. ***de intentie van het botnet?***
b. ***de commandostructuur van het botnet?***

Indien één van bovenstaande indelingen wordt gehanteerd, per indeling:

I.9.1. ***Komt de gehanteerde indeling overeen met de taxonomie van het referentiemodel? Waar zitten de verschillen?***

DefCERT maakt geen specifiek onderscheid tussen verschillende verschijningsvormen van botnets. DefCERT maakt voor alle malware, dus niet uitsluitend botnets, onderscheid in kwetsbaarheden die worden uitgebuit.

I.9.2. ***Wat voor botnetindeling, -classificatie of -taxonomie hanteert uw organisatie?***

DefCERT maakt op hoofdlijn onderscheid in de volgende dreigingen:

- social engineering;
- specifieke kwetsbaarheden van systemen;

- misbruik van in beginsel normale software voor computer- en netwerkbeheer.

I.9.3. ***Wat zijn de redenen om voor een dergelijke indeling te kiezen?***

DefCERT heeft primair een defensieve rol en wil in de eerste plaats de mogelijke kwetsbaarheden van Defensiesystemen kennen.

3.2. Botnetbestrijdingsmethoden

I.10. ***Op welke wijze of met welke methoden bestrijdt uw organisatie botnets? Met andere woorden: hoe gaat uw organisatie te werk?***

I.10.1. ***Bij wat voor soort botnets (conform de besproken classificatie) past u deze bestrijdingsmethode toe?***

DefCERT gebruikt de volgende bestrijdingsmethoden voor alle soorten botnets:

- kwetsbaarheid weghalen afhankelijk van dreigingbeeld / trendanalyse.
- verwijderen van botnets op eigen (Defensie) netwerken, evt. met (eigen) signatures.

DefCERT past geen van de andere methoden uit het referentiemodel toe, omdat het geen taak en bevoegdheden heeft om botnets actief te bestrijden door het aangrijpen van de commandostructuur van een botnet of de botmaster zelf.

I.10.2. ***Richt deze methode zich (primair) op individuele bots, de structuur van het botnet of tegen de botmaster?***

De toegepaste methode richt zich uitsluitend tegen individuele malware.

I.10.3. ***Komen de gehanteerde bestrijdingsmethoden overeen met de methoden in het referentiemodel? Waar zitten de verschillen?***

[*Conclusie van de interviewer aan de hand van antwoorden op zijn vragen naar specifieke aspecten in het referentiemodel: De eerste methode, nl. het weghalen van kwetsbaarheden is geen onderdeel van het referentiemodel, omdat het onderzoek zich niet op preventie richt. De tweede methode is wel één van de in het referentiemodel onderkende methoden voor botnetbestrijding.*]

4. Organisatie van botnetbestrijding

Per bestrijdingsmethode:

I.11. ***Over welke competenties (informatie, kennis, vaardigheden en middelen) beschikt uw organisatie om de bestrijdingsmethode toe te kunnen passen?***

Per competentie:

I.11.1. ***Zit er enige wettelijke restrictie op de aanwending van de competentie? Zo ja, is uw organisatie wettelijk bevoegd de competentie aan te wenden?***

I.11.2. ***In welke situaties, bijvoorbeeld bij wat voor soort botnet (naar oogmerk, commandostructuur of andere indeling) maakt u gebruik van de competentie?***

DefCERT beschikt over de volgende competenties ten aanzien van botnetbestrijding:

C1. Het detecteren van bots en botnets op internet met een honeynet.

C2. Het detecteren van bots en botnets op een specifiek netwerk met passieve methoden.

C3. Het onderzoeken van specifieke malware (software van botagents) op gedrag en eigenschappen.

C4. Het onderzoeken van de eigenschappen en het gedrag van specifieke botnets met behulp van een honeynet en door afvangen van botnetdataverkeer

C6. Het verwijderen van botagents van computers (op een eigen netwerk).

C9. Het verstoren of blokkeren van het botnet door manipulatie van de communicatie (op eigen netwerk).

C10. Het overnemen van het botnet door manipulatie van de communicatie.

C11. Het traceren van adressen / computers op internet.

Er zijn geen wettelijke beperkingen of bijzondere bevoegdheden nodig voor het aanwenden van deze competenties. DefCERT gebruikt deze competenties in principe voor alle soorten botnets.

I.11.3. ***Komen de competenties en bevoegdheden overeen met de die van het referentiemodel? Zo nee, waar zitten de verschillen?***

[*Conclusie van de interviewer aan de hand van antwoorden op zijn vragen naar specifieke aspecten in het referentiemodel: DefCERT is ook in staat adressen / computers op internet te traceren, terwijl dat volgens het referentiemodel niet noodzakelijk is bij de bestrijding van individuele bots.*]

I.12. ***Voor welke aspecten van botnetbestrijding beschikt uw organisatie niet over de benodigde bevoegdheden of competenties?***

I.13. ***Met welke organisaties wordt wegens een (gedeeltelijk) gebrek aan competenties of bevoegdheden samengewerkt?***

Per externe organisatie waarmee wordt samengewerkt:

I.13.1. ***Welke bevoegdheden en competenties die de externe organisatie heeft of zou moeten hebben, betreft het?***

DefCERT is weliswaar in staat zelf malware te onderzoeken en signatures te genereren, maar voor het merendeel van de passieve methoden voor botnetdetectie op Defensie-netwerken (C2) is DefCERT afhankelijk van antivirussoftware van private computerbeveiligingsbedrijven en beschikbare signatures.

DefCERT is niet in staat of bevoegd tot het achterhalen van encryptiesleutels en ontcijferen van informatie (C5). Hiervoor zou DefCERT afhankelijk zijn van de MIVD, maar de MIVD zet deze competentie niet in ten behoeve van DefCERT.

I.13.2. ***Indien het gaat om een gebrek aan bevoegdheden: worden eigen competenties aangewend onder auspiciën van een externe bevoegde organisatie, of maakt de externe organisatie bij de uitoefening van haar bevoegdheden gebruik van eigen competenties?***

Niet van toepassing: er is geen gebrek aan bevoegdheden voor aanwending van de benodigde competenties voor de taakstelling van DefCERT.

I.13.3. ***Beoordeelt u de samenwerking met de externe organisatie als effectief? Zo nee, waarom niet?***

I.13.4. ***Heeft de externe organisatie bepaalde bevoegdheden en/of competenties niet, die die organisatie wel zou moeten hebben om effectief te zijn? Zo ja, welke?***

De samenwerking met andere CERTs is goed. Er is voldoende informatie-uitwisseling om effectief te kunnen optreden.

De samenwerking met de MIVD is voor DefCERT niet effectief; omdat het vooral eenrichtingsverkeer is. De MIVD deelt geen informatie met DefCERT, waardoor er voor DefCERT geen synergie optreedt.

5. Effectiviteit van botnetbestrijding in Nederland

I.14. ***Zijn de verschillende organisaties die zich in Nederland met botnetbestrijding bezig houden in staat dat effectief te doen?***

Zo ja:

I.14.1. ***Waar blijkt dat naar uw mening uit?***

Ja, op het gebied van botnetbestrijding kan Nederland effectief optreden. Dat blijkt uit een goede publiek-private samenwerking, bijv. bij de Diginotar case waarbij DefCERT-specialisten het NCSC hebben ondersteund. In dergelijke bijzondere cases worden organisatorische grenzen opzij gezet zodat de juiste experts kunnen worden ingezet.

Zo nee:

I.14.2. ***Zijn er bestrijdingsmethoden die, door gebrek aan competenties, bevoegdheden of om andere redenen, niet in praktijk kunnen worden gebracht? Zo ja, welke?***

Nee, vanuit het perspectief van DefCERT zijn er geen bestrijdingsmethoden die niet in de praktijk kunnen worden gebracht. Daarbij opgemerkt dat DefCERT zich beperkt tot de bestrijding van bots/botagents; actieve vormen van bestrijding passen niet in de taak en opzet van een CERT-organisatie.

I.14.3. ***Zijn er soorten botnets die naar uw mening daarom niet (afdoende) kunnen worden bestreden?***

Nee.

Hoogstens zou de kennis over botnets, of malware in het algemeen, die zich richt op industriële systemen, (Supervisory Control And Data Acquisition, SCADA) moeten worden verbreed.

I.15. ***Zijn er naast de competenties en bevoegdheden nog andere aspecten die belangrijk zijn voor botnetbestrijding, maar die in het interview onderbelicht zijn gebleven?***

Geïnterviewde is van mening dat er veel low-tech manieren bestaan om een botnet op te zetten; botnetbestrijding zou dus primair in het tegengaan van de verspreiding van een botnet moeten liggen.

6. Afsluiting van het interview

6.1. Slotvragen

I.16. ***Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?***

Geïnterviewde laat weten dat zijns inziens, door de onbekendheid en beperkte kennis van de materie, een diffuus beeld kan worden gecreëerd door media en beleidmakers: ‘cyber’ als hype leidt af van de kern van botnetbestrijding.

6.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn tijd en medewerking

Appendix 5. Fox-IT

1. Inleiding

Dit is het verslag van het onderzoeksinterview afgenomen met Fox-IT op 23 mei 2013 te Driebergen. Het interview maakt deel uit van een afstudeeronderzoek aan de Faculteit Informatica van de Open Universiteit. Het onderzoek richt zich op de botnetbestrijding in Nederland. Het doel van dit interview is om op systematische wijze te inventariseren over welke competenties en bevoegdheden private partijen beschikken om verschillende soorten botnets te kunnen bestrijden.

2. Algemene vragen over de organisatie

2.1. Geïnterviewden

I.1.1. ***Wat is uw naam (incl. voorletters, evt. rang en titels)?***
I.1.2. ***Wat is uw functie / relatie tot botnetbestrijding?***
I.1.3. ***Tot welke organisatie behoort u?***

Dhr. Ronald Prins, directeur Fox-IT. Fox-IT is een computerbeveiligingsbedrijf dat overheidsorganisaties en vitale bedrijven als klant heeft, en als zodanig op verschillende wijzen is betrokken bij de beveiliging tegen cyberaanvallen, waaronder botnets.

2.2. Organisatie

I.2. ***Wat is de volledige naam van de organisatie? Wordt dit afgekort of zijn er andere aanduidingen voor de organisatie?***
I.3. ***Hoe is op hoofdlijnen de organisatie ingericht? Maakt de organisatie deel uit van een grotere organisatie?***
I.4. ***Indien van toepassing: wat is de rechtsbasis waaraan de organisatie haar bestaan en taken ontleent?***
I.5. ***Zijn er relevante openbare publicaties, zoals rapporten en jaarverslagen, van en over uw organisatie beschikbaar waarin cyber security in het algemeen of botnetbestrijding in het bijzonder aan de orde komen?***

Fox-IT is een privaat bedrijf met ongeveer 200 werknemers.
Op haar internetsite is de missie van de organisatie als volgt verwoord:

Fox-IT heeft als doel technische en innovatieve oplossingen te maken die voor een veiligere samenleving zorgen. Wij doen dit door geavanceerde diensten en oplossingen op het gebied van cyberbeveiliging en cyberdefensie te ontwikkelen voor onze klanten over de gehele wereld. Om dit te bewerkstelligen richten wij ons sterk op innovatie en zijn wij enorm toegewijd aan onze klanten, onze waarden en onze integriteit. Terwijl vooruitgang in de IT steeds meer mogelijkheden biedt voor misbruik door steeds geraffineerdere cybercriminelen en terroristen, zorgen de oplossingen van Fox-IT ervoor dat criminelen beter in de gaten kunnen worden gehouden, en kunnen worden opgespoord en vervolgd, en dat het beveiligingsniveau van vitale IT-netwerken en IT-systemen verhoogd wordt. Wij richten ons op de gebieden waar de systemen het meest kwetsbaar zijn en op sectoren waar veiligheid van cruciaal belang is. Hierbij valt te denken aan systemen voor de overheid tot op het niveau van 'staatgeheim' en de vitale infrastructuur, zoals de energiesector en banken.

Los van de organisatiestructuur met typische bedrijfselementen als marketing, sales etc., vinden de activiteiten van de organisatie op drie niveaus plaats: Strategie, Operations en Infrastructuur.

De infrastructuuractiviteiten richten zich op hardware- en netwerkoplossingen, zoals cryptografie en datadiodes. Operations houdt zich bezig met incident response, forensisch onderzoek etc. De strategieactiviteiten richten zich vooral op consultancy en computerbeveiligingsbeleid.

Fox-IT heeft als bedrijf reguliere jaarverslagen. Overige openbare informatie is in principe op de website van Fox-IT te vinden.

2.3. Andere organisaties

I.6. ***Welke andere organisaties die zich bezighouden met botnetbestrijding in Nederland zijn u bekend?***

Per bekende organisatie:

I.6.1. ***Wat is de naam van die organisatie?***
I.6.2. ***Wat voor soort organisatie betreft het?***
I.6.3. ***Publieke organisatie?***
I.6.4. ***Private organisatie: internetaanbieder / beveiligingsbedrijf / vitaal bedrijf / anders?***
I.6.5. ***Werkt u ook samen met die organisatie? Ad hoc of structureel?***

I.7. ***Met welke internationale organisaties werkt u samen?***

Fox-IT werkt samen met verschillende publieke organisaties binnen de overheid, variërend van de inlichtingendiensten tot de krijgsmacht. Een belangrijk onderdeel daarvan is samenwerking op infrastructuurgebied, zoals cryptografische oplossingen en datadiodes. Dit is een meer structurele samenwerkingsvorm. De samenwerking op strategisch gebied, bijvoorbeeld met NCSC is ad hoc en informeler.

Daarnaast zijn vitale bedrijven (banken, telecommunicatiebedrijven, energiesector) de belangrijkste klanten van Fox-IT. Deze samenwerking is meer ad hoc en richt zich vooral op incident respons. Deze samenwerking moet een meer structureel karakter krijgen en zich ook op meer strategische consultancyactiviteiten richten.

De samenwerking met aanbieders van internet en computerdiensten (Internetproviders en Hostingproviders) is erg beperkt, omdat zij een gering (commercieel) belang hebben bij botnetbestrijding en zich hoofdzakelijk richten op eigen beveiliging, hoewel ze in beginsel wel waardevolle informatie zouden kunnen verstrekken.

Fox-IT heeft zowel nationale als internationale klanten.

3. Botnetclassificatie en -bestrijdingsmethoden

3.1. Botnetclassificatie

I.8. ***Gebruikt uw organisatie een indeling, classificatie of taxonomie om verschillende soorten botnets te onderscheiden?***
I.9. ***Zo ja, is dit een indeling, classificatie of taxonomie gebaseerd op:***
a. ***de intentie van het botnet?***
b. ***de commandostructuur van het botnet?***

Indien één van bovenstaande indelingen wordt gehanteerd, per indeling:

I.9.1. ***Komt de gehanteerde indeling overeen met de taxonomie van het referentiemodel? Waar zitten de verschillen?***

Indien een andere indeling, classificatie of taxonomie wordt gehanteerd:

I.9.2. ***Wat voor botnetindeling, -classificatie of -taxonomie hanteert uw organisatie?***
I.9.3. ***Wat zijn de redenen om voor een dergelijke indeling te kiezen?***

Fox-IT hanteert geen indeling naar intentie van het botnet of de commandostructuur, zoals weergegeven in het referentiemodel. Op de eerste plaats is bij het grootste deel van de botnets sprake van een structuur met een centrale commandoserver. De complexere vormen komen slechts beperkt voor omdat de pakkans toch erg klein is en dus de complexiteit van complexere structuren daar niet tegen opweegt. Met andere woorden: botnets met een centrale commandoserver zijn ondanks hun relatieve eenvoud praktisch gezien goed genoeg in stand te houden voor een botmaster.

De intentie van het botnet is wel relevant voor welke (overheids)organisatie uiteindelijk primair de regie over de bestrijding heeft, maar is voor een private organisatie als Fox-IT niet relevant voor hoe zij de

bestrijding aanpakt wanneer zij wordt ingehuurd. Bovendien kan de intentie van een botnet veranderen naarmate de botmaster het botnet ter beschikking stelt aan andere partijen.

3.2. Botnetbestrijdingsmethoden

I.10. ***Op welke wijze of met welke methoden bestrijdt uw organisatie botnets? Met andere woorden: hoe gaat uw organisatie te werk?***

- I.10.1. ***Bij wat voor soort botnets (conform de besproken classificatie) past u deze bestrijdingsmethode toe?***
- I.10.2. ***Richt deze methode zich (primair) op individuele bots, de structuur van het botnet of tegen de botmaster?***
- I.10.3. ***Komen de gehanteerde bestrijdingsmethoden overeen met de methoden in het referentiemodel? Waar zitten de verschillen?***

Het overnemen en uitschakelen van commandoservers door Fox-IT (namens een klant die wordt aangevallen door een botnet) is in beginsel mogelijk. Wettelijk gezien ontbreekt daar de (expliciete) bevoegdheid voor, maar het is een grijs gebied. Als hiermee een serieuze dreiging voor een vitaal bedrijf kan worden weggenomen, is het de vraag of ingrijpen door een private partij daadwerkelijk als wederrechtelijk moet worden beschouwd. Verstoring door manipulatie van communicatie kan in beperkte mate op bedrijfsnetwerken (van klanten), maar de internetaanbieders zouden dit gerichter en grootschaliger kunnen doen.

Het aangrijpen van de botmaster (vervolging, arrestatie, uitschakeling) is voor een private partij geen effectieve bestrijdingsmethode, omdat de eerste prioriteit ligt bij het wegnemen van de aanval of de dreiging, en bij het opheffen van de verstoringen.

4. Organisatie van botnetbestrijding

I.11. ***Over welke competenties (informatie, kennis, vaardigheden en middelen) beschikt uw organisatie om de bestrijdingsmethode toe te kunnen passen?***

Per competentie:

- I.11.1. ***Zit er enige wettelijke restrictie op de aanwending van de competentie? Zo ja, is uw organisatie wettelijk bevoegd de competentie aan te wenden?***
- I.11.2. ***In welke situaties, bijvoorbeeld bij wat voor soort botnet (naar oogmerk, commandostructuur of andere indeling) maakt u gebruik van de competentie?***
- I.11.3. ***Komen de competenties en bevoegdheden overeen met de die van het referentiemodel? Zo nee, waar zitten de verschillen?***

I.12. ***Voor welke aspecten van botnetbestrijding beschikt uw organisatie niet over de benodigde bevoegdheden of competenties?***

I.13. ***Met welke organisaties wordt wegens een (gedeeltelijk) gebrek aan competenties of bevoegdheden samengewerkt?***

Per externe organisatie waarmee wordt samengewerkt:

- I.13.1. ***Welke bevoegdheden en competenties die de externe organisatie heeft of zou moeten hebben, betreft het?***
- I.13.2. ***Indien het gaat om een gebrek aan bevoegdheden: worden eigen competenties aangewend onder auspiciën van een externe bevoegde organisatie, of maakt de externe organisatie bij de uitoefening van haar bevoegdheden gebruik van eigen competenties?***

C1. Het detecteren van bots en botnets op internet met een honeynet.
C2. Het detecteren van bots en botnets op een specifiek netwerk met passieve methoden.

Een private partij als een computerbeveiligingsbedrijf is vrijer in het detecteren en onderzoeken van botnets met een honeynet dan de politie, die alleen gericht onderzoek mag doen. Het detecteren van botnets op een specifiek netwerk met passieve detectiemethoden is primair een aangelegenheid van de

eigenaar van die netwerken, die daarvoor gebruik kan maken van computerbeveiligingsbedrijven en deze dienst kan uitbesteden.

Geïnterviewde wijst erop dat detectie van botnets vaak niet met specifieke detectiemethoden voor botnets plaatsvindt, maar omdat er andere aanwijzingen zijn, zoals het daadwerkelijk ervaren van een aanval, of verdachte financiële transacties, etc.

C3. Het onderzoeken van specifieke malware (software van botagents) op gedrag en eigenschappen.

Dit wordt door geïnterviewde gezien als een typische kerncompetentie voor specifiek daarop gerichte computerbeveiligingsbedrijven, zoals antivirusbedrijven.

C4. Het onderzoeken van de eigenschappen en het gedrag van specifieke botnets.

De aanwending van deze competenties is erg contextafhankelijk, maar wanneer het computerbeveiligingsbedrijf Fox-IT wordt ingehuurd, wordt het botnet met verschillende voor de hand liggende middelen onderzocht om de dreiging in kaart te brengen en te bestrijden.

C5. Het achterhalen van encryptiesleutels en ontcijferen van informatie.

Ja, daar is Fox-IT toe in staat, waarbij wordt aangetekend dat in het algemeen de vercijfering ofwel te eenvoudig te kraken is (bijvoorbeeld omdat sleutels hardcoded zijn en met reverse engineering snel achterhaald kunnen worden), ofwel te moeilijk is.

C6. Het verwijderen van botagents van computers (op een netwerk van een klant).

Dit is in beginsel aan (vitale) bedrijven zelf, met behulp van daarvoor ontwikkelde software van gespecialiseerde computerbeveiligingsbedrijven voor antivirussoftware.

C7. Het overnemen van een commandoserver.

Het overnemen en uitschakelen van commandoservers door Fox-IT (namens een klant die wordt aangevallen door een botnet)is in beginsel mogelijk. Wettelijk gezien ontbreekt daar de (expliciete) bevoegdheid voor, maar het is een grijs gebied. Als hiermee een serieuze dreiging voor een vitaal bedrijf mee kan worden weggenomen, is het de vraag of ingrijpen door een private partij daadwerkelijk wederrechtelijk is of als zodanig moet worden gezien. Verstoring door manipulatie van communicatie kan in beperkte mate op bedrijfsnetwerken van klanten, maar de internetaanbieders zouden dit gerichter kunnen doen.

C8. Het verstoring van het botnet met gemanipuleerde bots.

Botnets zijn momenteel nog vrij eenvoudig in structuur, waardoor deze complexere competentie op dit moment weinig meerwaarde biedt.

C9. Het verstoren of blokkeren van het botnet door manipulatie van de communicatie.

Dit is een kerncompetentie voor internetaanbieders die primair de communicatie- en netwerkinfrastructuur van het internet beheren, maar ook vitale bedrijven kunnen dit op hun eigen netwerken uitvoeren.

C10. Het overnemen van het botnet door manipulatie van de communicatie.

Botnets zijn momenteel nog vrij eenvoudig in structuur, waardoor deze complexere competentie op dit moment weinig meerwaarde biedt.

C11. Het traceren van adressen / computers op internet; EN
C12. Het regulier opsporen van de botmaster:
   a. door opsporingsinstanties in Nederland;
   b. met medewerking van autoriteiten in het buitenland.

Hier geldt dat in veel gevallen, met gebruik van verschillende (open) bronnen, het achterhalen van de botmaster effectiever is dan tracering via de gebruikte netwerkpaden op het internet.

C13. Het in beslag nemen van een commandoserver / computermateriaal.

Private instanties kunnen via de rechter beslag laten leggen op een server, maar dat is praktisch gezien een omslachtige en een weinig effectieve methode, omdat het de botmaster zich of in het buitenland bevindt of met een andere server het botnet kan aansturen.

C14. Het veiligstellen van bewijsmateriaal (zowel fysiek als digitaal).

Fox-IT is in staat bewijsmateriaal veilig te stellen en digitaal te onderzoeken, al dan niet voor eigen gebruik of strafrechtelijke opsporing.

C15. Het arresteren en vervolgen van de botmaster(s).

Geen taak voor een private partij, en voor private partijen ook geen prioriteit.

C16. Op bijzondere wijze opsporen van de botmaster in het buitenland.
C17. Het fysiek uitschakelen van botmaster(s) en/of infrastructuur.

Geen taak voor een private partij.

Geen taak voor een private partij.

Overige competenties:

C18. Samenwerking en coördinatie voor botnetbestrijding.

Is primair een overheidstaak, waarbij het wel van belang is niet méér coördinerende instanties te creëren, maar de bestaande instanties op ieder van hun terreinen effectief te laten samenwerken. Dat wil zeggen: bij een botnetdreiging snel een gezamenlijke eerste analyseslag maken, om vervolgens de regie zo snel mogelijk over te dragen aan de meest geschikte partij.

C19. (Wetenschappelijk) onderzoek (ten behoeve van alle andere competenties) op het gebied van botnetbestrijding.

Ja, Fox-IT doet onderzoek en vergaart inlichtingen. Structureel onderzoek en trendanalyse zouden wel meer onderling moeten worden afgestemd met de overheid en andere partijen.

I.13.3. ***Beoordeelt u de samenwerking met de externe organisatie als effectief? Zo nee, waarom niet?***

Voor de eigen taakuitvoering wel, maar in bredere context is de kans dat een botmaster wordt gepakt, of een botnet wordt ontmanteld, te klein om een botmaster af te schrikken.

I.13.4. ***Heeft de externe organisatie bepaalde bevoegdheden en/of competenties niet, die die organisatie wel zou moeten hebben om effectief te zijn? Zo ja, welke?***

Als de overheid wil vasthouden aan het monopolie om geweld te gebruiken en/of in bepaalde gevallen inbreuk te maken op de rechten van derden (bijvoorbeeld het binnendringen van een computer), dan moet ze ook bereid zijn die middelen daadwerkelijk aan te wenden om effectieve bestrijding mogelijk te maken. In het geval van botnets is het overnemen of uitschakelen de meest snelle en effectieve methode voor de meest voorkomende botnets.

5. Effectiviteit van botnetbestrijding in Nederland

I.14. ***Zijn de verschillende organisaties die zich in Nederland met botnetbestrijding bezig houden in staat dat effectief te doen?***

Zo ja:

I.14.1. ***Waar blijkt dat naar uw mening uit?***

Zo nee:

I.14.2. ***Zijn er bestrijdingsmethoden die, door gebrek aan competenties, bevoegdheden of om andere redenen, niet in praktijk kunnen worden gebracht? Zo ja, welke?***
I.14.3. ***Zijn er soorten botnets die naar uw mening daarom niet (afdoende) kunnen worden bestreden?***

I.15. ***Zijn er naast de competenties en bevoegdheden nog andere aspecten die belangrijk zijn voor botnetbestrijding, maar die in het interview onderbelicht zijn gebleven?***

In zijn algemeenheid worden botnets onvoldoende bestreden. Het is belangrijk te beseffen dat de mogelijkheden voor passieve bestrijding en preventie (binnen redelijke grenzen) zijn uitgeput. Zolang het

gebruik van botnets loont, en ongehinderd en ongestraft blijft, zal de dreiging aanhouden en blijven de risico's groot. Actieve bestrijding is belangrijk om het gebruik van botnets minder aantrekkelijk te maken.

6. Afsluiting van het interview

6.1. Slotvragen

I.16. ***Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?***

De geïnterviewde heeft geen aanvullende opmerkingen.

6.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking en het interessante gesprek. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek.